Ying *et al. J Surveill Secur Saf* 2023;4:112-28
DOI: 10.20517/jsss.2023.26

Journal of Surveillance, Security and Safety

Original Article

Open Access

Check for updates

Blockchain distributed identity management model for cross-border data privacy protection

Zuobin Ying, Kaichao Wang

Faculty of Data Science, City University of Macau, Macau 999078, China.

Correspondence to: Kaichao Wang, Faculty of Data Science, City University of Macau, Macau 999078, China. E-mail: D22091101700@cityu.mo

How to cite this article: Ying Z, Wang K. Blockchain distributed identity management model for cross-border data privacy protection. *J Surveill Secur Saf* 2023;4:112-28. http://dx.doi.org/10.20517/jsss.2023.26

Received: 6 Aug 2023 **First Decision:** 25 Sep 2023 **Revised:** 8 Nov 2023 **Accepted:** 23 Nov 2023 **Published:** 11 Dec 2023

Academic Editors: Bomin Mao, Qiong Huang **Copy Editor:** Yanbin Bai **Production Editor:** Yanbin Bai

Abstract

Cross-border data privacy protection often involves personal privacy data from different regions, where cross-border vehicle identity authentication requires a large amount of sensitive data. The cross-border movement of this sensitive data poses a significant threat to privacy. A distributed identity management blockchain model for cross-border data privacy protection is proposed to avoid the cross-border transmission of sensitive data through identity authentication. The model combines the SM2 and SM9 algorithms and blockchain technology to guarantee the security of stored data while providing a method to avoid sensitive data crossing borders and realizing cross-border identity authentication. The model was originally designed for the Northbound Travel for Macao scenario but can still be applied to other cross-border authentications. The generation speed of a Non-Fungible Token is verified through experiments, and the generation time and efficiency of Non-Fungible Tokens satisfy the actual needs of Internet of Vehicles authentication.

Keywords: Cross-border Identification, Blockchain, SM9, SM2, NFT

1. INTRODUCTION

Cross-border data transfer refers to any action involving data transfer to another jurisdiction or the intention to transfer data again after it has been moved to another jurisdiction. Cross-border data privacy collection often involves gathering data with privacy implications from different regions, making it inherently complex. Given the potential involvement of overseas laws and regulations due to cross-border factors, conducting thor-

ough research and assessment should precede cross-border data collection to ensure compliance with various regional regulations and safeguard the security of personal data.

Take the data exchange in the Guangdong-Hong Kong-Macau Greater Bay Area as an example; personal health data is restrictively forbidden across the border. That is, if a person takes a nucleic acid test in Mainland China, they cannot show the result to the health department in Macau S.A.R., and vice versa.

Cross-border data may often encompass sensitive and private information, such as personal and business data. However, there are situations where a specific need for cross-border data transfer is unavoidable. Whether it is an emerging economic form, such as the sharing economy, new media, etc., or a traditional e-commerce platform, it is necessary to accumulate user data in business activities to improve business and service capabilities, which requires companies to gather data on a global scale[1].

In integrating the Guangdong-Hong Kong-Macao Greater Bay Area, cross-border vehicle data connectivity plays a crucial role. However, regarding the vehicle data exchange between Guangdong and Macao, collecting cross-border vehicle data requires strict compliance with all parties involved in regional cross-border data regulations. This is particularly crucial when the collected data involves personal and sensitive information, as obtaining authorization and consent from the data owners becomes necessary. Consequently, the scope of entities engaged in cross-border data collection activities will be more extensive. Government agencies and Internet of Vehicles (IoV) service providers in the vehicle industry will collect and utilize various types of data to regulate the management of Macao motor vehicles entering and exiting the Mainland.

The ubiquitous exchange of data across borders has given rise to concerns by governments and citizens about some of the adverse effects of so much personal data or personally identifiable information[2]. The current IoV security protection level cannot meet data security requirements, especially vehicle data analysis and response, which will further affect the braking choice for the vehicle. Once criminals tamper with or forge relevant data, it will affect vehicle and user safety and even threaten social security[3]. Hence, protecting cross-border data has become a challenging issue worthy of research, given the security risks associated with such data. It is not easy to safely manage data transfers since each respective country has separate data protection rules that are used for the governance of personal data[4].

This study aimed to prevent cross-border sensitive data using identity authentication while securing part of the non-sensitive cross-border data for privacy protection, mainly for the scenario of Northbound Travel for Macao (NTM). The model aims to facilitate the identification of Macao vehicles in Guangdong. Upon registering and driving their truck within Guangdong, the envisioned Macao vehicle owners only need to register their cell phone number and license plate number and then submit biometric information, such as their identity card, cell phone number, and license plate number, to the Macao Transport Bureau for registration. It is not necessary to give out too much personal information, including biometric data. The Guangdong Provincial Department of Transportation (GDOT) and the Macao Transport Bureau use the designated procedures of the program to verify user identity and then confirm it with the hash provided by Customs. Through verification of time locks and issuance of certificates, the private data of the vehicle owner is kept in Macau while achieving cross-border identity authentication, ensuring security and privacy.

The main issue addressed in this study is protecting the sensitive data of cross-border vehicles in the NTM system while simultaneously accomplishing identity authentication for NTM users. The difficulty of this scheme lies in the need to collect enough personal privacy data for user authentication while minimizing the transfer of the sensitive data across borders. Ultimately, there is also a necessity to ensure that both the cross-border and stored data are encrypted to prevent leakage.

First, we must solve the storage problem to collect user information necessary for completing the authentication. In the past, cross-border data often used cloud storage to store data, but cloud storage security can be problematic. Rahman *et al.* showed the blockchain-less use-case of cross-border data sharing to show the real-life necessity of blockchain. Data from different IoT devices are stored in the cloud. Such cloud-stored data is accessed from various regions/countries, but the data transaction information is not stored in the blockchain. In this case, malicious users may cause harm to the sensitive data[5]. Combining the various requirements above and considering the immutability of blockchain technology, we first identified the use of blockchain for data storage and querying.

Blockchain is an emerging technology with great potential given its security control mechanism, immutability, transparency, traceability, and reconciliation process, which already has created hype in various sectors, including healthcare, education, supply chain, and especially cross-border payment in the financial sector[6]. An advantage of blockchain technology is that it can guarantee perfect information while scientifically dealing with problems such as high cost, difficult accountability, and unclear processes[7]. To achieve searchable and tamper-proof data storage during the period, the user's private data must be encrypted and uplinked to generate Non-Fungible Tokens (NFTs).

An NFT is a cryptocurrency derived from Ether's intelligent contracts; it is a unique and non-interchangeable data encryption token stored on a unique blockchain. NFTs are suitable for uniquely identifying something or someone[8]. NFT technology has provided value to the uniqueness and scarcity of blockchain-based digital assets or real assets to guarantee ownership and trade them[9]. Powered by smart contracts deployed in different blockchains, NFTs have given content creators more control and power than ever before, giving birth to the core concept of verifiable digital ownership[10].

Although Bitcoin can provide some weak anonymity by using many identities (pseudonyms), the amount of money transferred in transactions (i.e., confidentiality) is public to everyone. This severe limitation makes Bitcoin unsuitable for confidential scenarios, such as a second-price auction, which requires confidentiality to incentivize truthful bidding[11]. Therefore, for privacy protection purposes, after using blockchain technology to meet the demand for non-comparability and queryability, it is necessary to use encryption algorithms to protect the cross-border data and the security of the data on the chain and realize the encryption and protection of the data.

We aim to solve the problem of sensitive data transmission across borders. Our proposed solution is as follows: after the user crosses the border, only part of their data will be transmitted back to their country of origin. This transmitted portion will be used to query the complete identity, which will verify the user's authentication in their country of origin. This will help us avoid most cross-border transmission of sensitive data. Although both parties have collected the personal information of vehicles and users, the collected data is stored locally and does not need to be transmitted in clear text across the border.

The last problem we want to solve is data storage; our model chooses to encrypt using the state cipher algorithm to prevent data leakage in on-chain data and cross-border transmission. In other regions, the encryption algorithm of this model can be replaced with different cryptographic algorithms.

Therefore, the basic idea of this scheme is to encrypt users' sensitive data and then upload it to generate an NFT, utilizing the blockchain platform for data storage and achieving queryability and non-tampering of the data. After that, the encryption algorithm is used to secure the data in the blockchain and the cross-border data, passing part of the data across borders to accomplish authentication. Ultimately, the Attribute-Based Encryption (ABE) algorithm is utilized to make the cross-border data decryptable only by the Trusted Authorities (TAs) of both parties.

The contributions of this study can be summarized as follows:

- The proposed model provides a secure cross-border authentication method to avoid cross-border transmission of sensitive user data through identity authentication while securely preserving user data.
- A distributed cross-border data privacy-preserving identity management model is proposed to address the above security challenges of cross-border data transmission security.
- The use of blockchain and NFT technology protects the user's identity data, which plays the role of authentication while preserving the user's data, using the state secret algorithm to achieve data encryption and protection.

2. RELATED WORK

Synthesizing the development and application of NFTs in recent years, our model selects them as the data storage and query method and generates NFTs for user data to ensure queryability and prevent tampering. Scholars have gradually emphasized the use of NFTs for authentication and recognition of identity in recent years; current NFTs are mainly applied to prove the ownership of virtual digital assets, such as videos, games, and images.

Mohan *et al.* designed and developed an immutable, decentralized, and transparent module credit management system based on the Ethereum blockchain and NFTs. The decentralized application (DApps) fulfilled the objective of allowing faculties to issue achievements/credits onto the blockchain and for students to view their achievements through the NFT-Merit system[12]. Tharun proposed a DApp of NFTs for the music industry based on blockchain smart contracts to maintain music copyright, ownership, and blockchain-based automated royalty distribution[13]. Takahashi *et al.* proposed a long-term storage node system architecture named Sustainable Generation Manager (SGM) to solve the problem of high cost consumed when using NFTs to store data[14].

In recent years, many scholars have worked to improve the utility of NFTs, address some of their shortcomings, and apply NFTs to other applications. Chen *et al.* proposed a new NFT model, a synergy of a new economic mechanism backed by game theory and two supplementary algorithms, to address the problem of poor copyright traceability of out-of-chain data[15]. Manzoor *et al.* proposed a novel NFT-based framework to bring high throughput and excellent scalability to blockchain-based applications using a "Proof-of-Stake" consensus algorithm based on blockchain technology for data transactions, validation, and resource management[16].

Bellagarda1 and Abu-Mahfouz addressed two problems by developing and demonstrating a theoretical workflow for a system that incorporates NFTs and verifiable credentials, presenting an academic workflow for the development of a system that includes NFTs and verifiable credentials in a decentralized manner to store the underlying NFT digital assets, as well as NFT infringement and fraud, which were discussed and addressed through the development of a practical application called Connect2NFT[17]. Sun *et al.* proposed a multi-chain aggregated identity scheme that uses cryptographic accumulators to improve efficiency significantly and provides a way for VASPs, such as centralized exchanges, to demonstrate Proof of Reserves (PoR) to users[18]. Wang *et al.* proposed a referable NFT (rNFT) scheme to improve the exposure and enhance the reference relationship of inclusive NFTs[19].

However, many scholars have worked on the use of NFTs for identity authentication. Khalil *et al.* proposed a decentralized smart city (DSCoT) architecture based on private blockchain to address the security issues of smart cities. They utilized NFTs to provide authentication functions for devices and users[20]. Neisse *et al.* proposed a blockchain-based platform using a novel cross-ledger design that addresses some of the main requirements of current EU cybersecurity legislation through interledger mechanisms. The advantages of blockchain

in distributed trust, transparency, and accountability are exploited while dealing with scalability, performance, and interoperability requirements[21]. The idea behind the above studies is to utilize a blockchain platform for distributed design while accomplishing authentication.

Similarly, some researchers have used NFTs for privacy protection. Peng *et al.* proposed BlockShare, a blockchain-based privacy-preserving verifiable data-sharing system. They designed a novel blockchain-based architecture and developed a zero-knowledge verification scheme. Experimental results show that BlockShare enables the verifiable sharing of personal data in a privacy-preserving manner[22]. Dang *et al.* proposed an approach to smart home data privacy protection based on blockchain technology using experimental scenarios with Ganache, Remix, and web3. They compared the proposed architecture with existing models. Their proposed architecture addresses the challenges of data privacy, trust access control, and scalability in smart home environments[23].

This article demonstrates the emergence of security solutions that use NFTs for authentication and privacy protection. It is feasible to leverage a blockchain platform to generate NFTs for authentication and privacy protection.

3. MODEL IMPLEMENTATION

3.1. System model

The model proposed in this paper is based on the generation and verification of NFTs and signature verification of data, which utilizes the verifiability and uniqueness of NFTs to authenticate users. The model requires three participants: the TA, User, and Digital Center (DC). A TA often refers to a widely recognized entity or organization that possesses credibility and authority and serves to enhance system security and provide authentication and authorization for both parties. A trusted Data Center often refers to a data center that is secure and reliable and and has a high degree of trust.

The TA is the authoritative entity that records and maintains user information, which refers to the Transport Bureau of Macao, the GDOT, and Customs in this study. Macau Transportation Bureau and the Department of Transport of Guangdong Province also serve as the two DCs in this project. A user is an entity with a Physical Identity (PID) and Decentralized Identifier (DID), referring to Macau car owners who travel from Macau to Guangdong Province under the Northbound Travel for Macau.

The cross-border vehicle data privacy collection in this model is a subset of cross-border data privacy collection. It refers to collecting data related to cross-border vehicles, often involving the personal privacy of vehicle owners, such as vehicle location, travel history, vehicle performance metrics, and owner identity information. These data elements can indeed be sensitive, potentially influencing the privacy of vehicle owners. Combining the various requirements above, we first decided to use the blockchain for the storage and querying of the data, and out of consideration for the region proposed in the project proposal (Macao-Guangdong), we first considered the national cryptographic algorithms. In the other areas, SM2 can be replaced with RSA and SM9 with different ABE algorithms to suit given needs.

In the model depicted in the flowchart in Figure 1, users are required to first submit their unique and unforgeable identity verification, such as personal information or biometric data, to one of the TAs. After this, the TA utilizes a part of this data to generate a Decentralized Part Identifier (DPID) and create a signature for the Vehicle Public Key Table (VPKT).

After the user crosses the border, part of the data uploaded to the original TA (part used to generate the DPID) is uploaded to the cross-border TA by the user themselves. The cross-border TA recalculates the DPID using

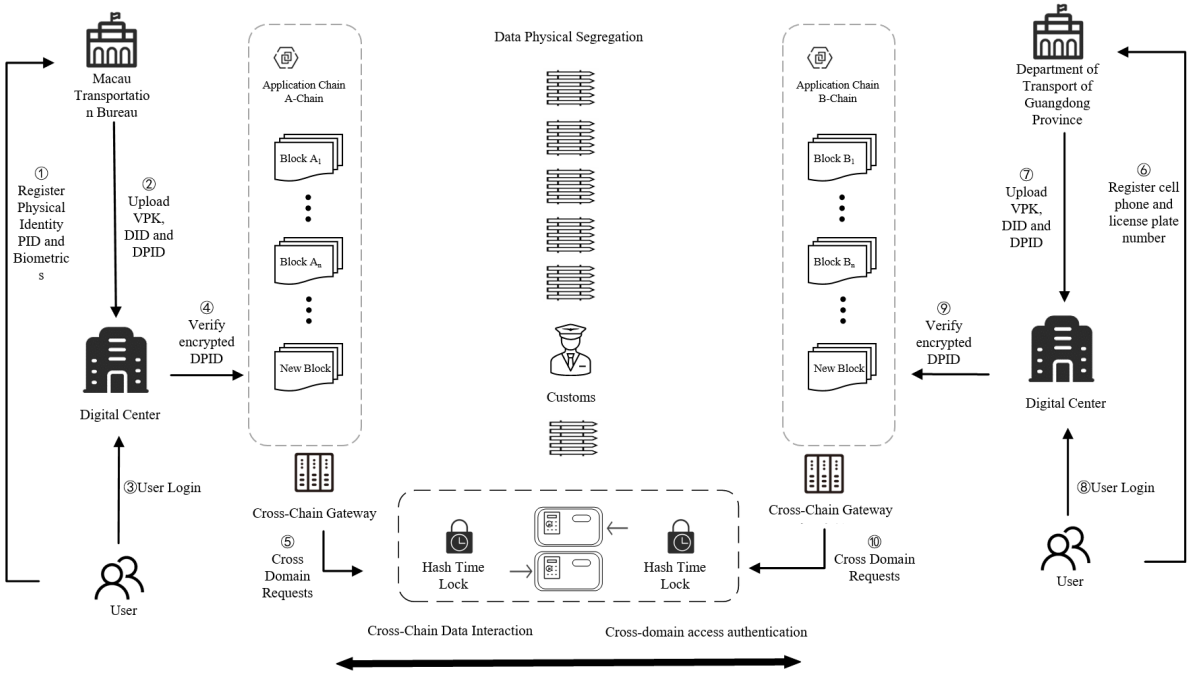

Figure 1. Distributed Identity Management Model Based on Blockchain.

the same encryption method, encrypts the DPID, and broadcasts it back to the original TA to search for the VPKT and authenticate. The cross-border TA must ensure that the encrypted DPID can be decrypted only by the original TA. After decrypting the broadcasted information, the original TA decrypts the DPID, further searches for the user's VPKT, and then can obtain the user's DID and finish the next authentication.

The program uses the SM9 algorithm as ABE encryption to ensure the security of cross-border data and utilizes the hash time lock and NFTs to authenticate the identity of both parties; at the same time, taking into consideration the lightweight use of IoV, the SM2 algorithm of the state secret is used to sign and verify the data on the NFT to ensure the safety of cross-border data. After successful SM2 verification, the cross-chain request is forwarded through the cross-chain gateway, and then, an identity audit is performed through the hash time lock. The clearance credentials are issued after the audit.

The proposed model is based on the NTM. Theoretically, it could be used for other cross-border authentication, especially for flows between two locations. According to the designed model, the solution can be realized in four steps.

3.2. Blockchain creation and initialization

The first step is the creation of the blockchain, where the TA first authenticates all blockchain managers and authorizes them to participate in the consensus process, with the Macau Transportation Bureau creating application chain A-Chain and the Department of Transport of Guangdong Province creating application chain B-Chain.

To start the transactions and verification required by the project, the TA needs to certify all blocks according to Practical Byzantine Fault Tolerance (PBFT) and authorize them to ensure the security of the blockchain creation.

After securing the blockchain, the next step for the TA is to activate the federated blockchain in the pre-

configured network nodes based on the consensus mechanism. A federated blockchain is participated in and managed by multiple organizations with a certain degree of openness and decentralization and is mainly used to maintain the blockchain. After the creation of the blockchain, it is necessary to initialize the system and set up an intermediate account on the application chain A-Chain to realize the data exchange business.

After the initialization of the application chain, the Macao Transportation Bureau and GDOT upload their user information to the VPKT of the application chain, i.e., A-Chain and B-Chain, respectively, and then verify the data flow through the hash time lock of Customs. The advantage of using a private chain is that if the encryption algorithm we chose is cracked in the future, the data stored on the private chain is guaranteed to be read only by the TA, which does not result in a serious privacy breach.

3.3. Smart contract deployment and initialization

The next step is to deploy the required smart contracts on the established blockchain. A special function of blockchain technology is a smart contract, which is transparent and unchangeable[24]. Smart contracts are usually user programs, algorithms, or protocols that can be used to verify, validate, or make irreversible transactions[25]. Controlling the operation of the blockchain by writing the code for smart contracts allows the blockchain to run without third-party execution after certain conditions are met, which plays a vital role in the blockchain.

The smart contract in this project is mainly applied to the TA, which allows the TA to call the VPKTA algorithm by using the Application Binary Interfaces (ABIs) provided by the smart contract to initialize, add, and delete VPKTs in the smart contract and similarly to complete the generation of NFTs and uploading of data.

Considering the above requirements, the smart contract needs to invoke the Initialization algorithm in the VPKT Algorithm (VPKTA) to declare the structure of the VPKT elements in the smart contract and the transactions initialized in the smart contract to specify the query format. In writing intelligent contracts, functions must be written according to the required algorithm for invocation. Considering that some parts, such as the generation of NFTs, require the execution of the blockchain, more than one smart contract may be necessary for the whole project, and the deployment and invocation of intelligent contracts are also required.

For example, the TA uses the call function to realize the use of the updateVPKT algorithm to update the public key that already exists in the VPKT or uses the revokeVPKT algorithm to revoke the vehicle in the VPKT in the relevant items to achieve the generation of the NFT, deployed after the call of the NFT contract.

The initialization of the TA is mainly to initialize the content required by the ABE algorithm, including the generation of the initial parameters of Elliptic Curve Cryptography (ECC) and the age of the master key and subkeys. In this stage, the TA will carry out the first step using ECC, a kind of asymmetric encryption algorithm based on the mathematical theory of elliptic curves. ECC is an asymmetric encryption algorithm based on the mathematical theory of elliptic curves, which can use shorter keys to achieve comparable or higher security than RSA.

The above is the preparation of the system; after the TA and DC have done the above preparatory work, they can interact with the user to carry out the actual registration and authentication processes, etc.

3.4. SM9-Based authentication

As the parties involved in this project are situated in Guangdong and Macau, we selected SM9 as the ABE algorithm to be employed. This choice ensures that the encryption and decryption of data can only be carried out between the TA parties, providing a secure solution.

SM9 is a class of identity-based cryptography schemes based on pairing published by the State Cryptography Administration of China in 2016. It includes four parts: digital signature, data encryption, key exchange, and key encapsulation schemes[26]. The SM9 algorithm is a high-intensity asymmetric encryption algorithm; its strength on the standard selected reference curve is equivalent to that of RSA-3072 bit security[27].

The SM9 asymmetric algorithm is one of the core algorithms independently mastered in China. Its security is comparable to that of SM2, RSA, and other algorithms. It plays a vital role in improving the safety performance of equipment on the power data collection terminals, such as data gateway machines and monitoring devices[28]. The role of SM9 in this project is to act as an ABE algorithm to protect the privacy of specific data across borders, using the public key encryption of SM9 to encrypt DPID to generate masked identities to ensure only the application chain A-Chain (B-Chain) can decrypt them.

Figure 2 shows a flowchart of the encryption and decryption given in the SM9 digital signature algorithm[29], where the message to be sent is a bit string M, men (the bit length of M), K1-len (the bit length of the key K1 in the packet cipher algorithm), K2-len (the bit length of the key K2 in the function MAC), and Hv (), which is a cryptographic hash function used in the bilinear pairwise computation and hash algorithm. The master key and token encrypt the DPID of the vehicle, and the encrypted data require the ticket and encrypted private key to complete the decryption, which realizes the requirements of the ABE algorithm in the scheme. The encrypted private key needs to be generated by KGC based on the combination of the encrypted master key and token of both parties; in this project, it is realized by the trusted DC of both parties.

After completing public key encryption and decryption, both parties must exchange keys and negotiate, including exchanging system parameters and agreeing on a new key. In this process, it needs to be ensured that only the responding party that has mastered the encryption private key can complete the negotiation. SM9 uses the intractability of bi-directional pairs in the elliptic curve to realize a symbol-based secret key exchange negotiation, and both parties need to agree on a secret key by using symbols and the encryption private key, using this process to complete the key exchange. This process completes the critical discussion. The essential exchange parties in the project are the cross-border TA and original TA, and both parties can negotiate a secret key for them to use in other algorithms through this process.

A flowchart of key exchanges in SM9 is shown in Figure 3[29]:

The initiating user A and responding user B participating in the critical exchange hold an identification and corresponding encrypted private key generated by the key generation center through the combination of the encrypted master secret key and the user's identification. Users A and B here correspond to the Macao Transportation Affairs Bureau (MTA) and GDOT in the project, respectively. Users A and B agree on a secret key known only to them through interactive messaging with their identities and respective encrypted private keys, and both users can optionally realize essential confirmation. This shared secret key is usually used in a symmetric cryptographic algorithm. The key exchange protocol can be used for key management and negotiation, which both parties in the project can accomplish through the gateway.

To ensure the security of the key during transmission, specific encapsulation of the key is also required. The key encapsulation algorithm requires the encrypting party to use the encrypted master key and identification of user B; the encapsulating party and the receiving party encrypt and decrypt the key through the user's authentication and encrypted private key, respectively, to ensure that only the receiving party can complete the decryption to get the encapsulated key so that the encrypted master key and encapsulated key can be realized by the two-party exchange and the encapsulated key can further ensure the security of the information.

The complete flowchart of the SM9 algorithm standard is shown in Figure 4[29].

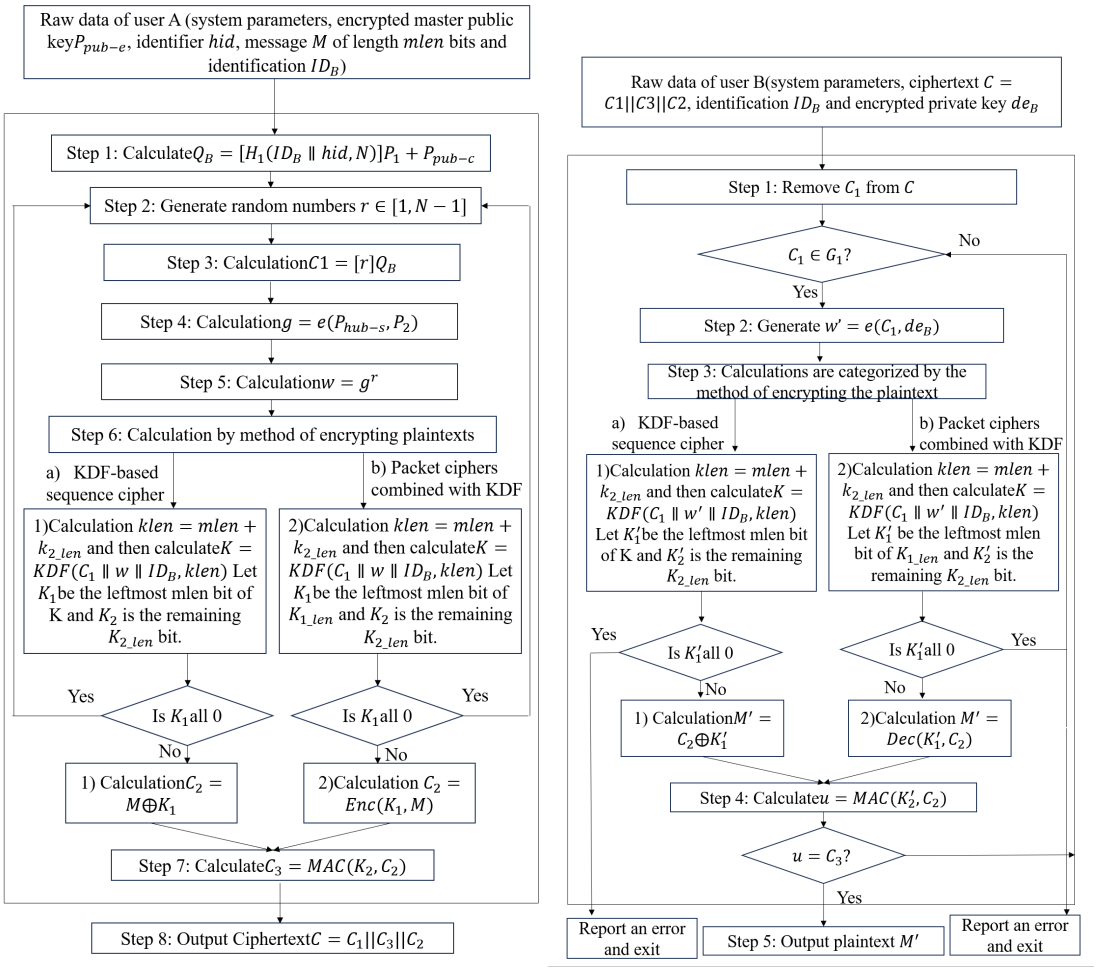

Figure 2. SM9 Public Key Encryption and Decryption Algorithm Flow.png.

Above, we use the SM9 algorithm to allow both data centers to securely exchange masked identities of DPIDs broadcasted to the outside world to ensure data privacy protection across the blockchain.

3.5. SM2-Based NFT authentication

The SM2 algorithm is based on the elliptic curve cipher mechanism 256-bit cipher with high efficiency and high security, commonly used in data encryption.

In the flow of the model, the user logs in through password and biometric authentication after crossing the border to provide the cross-border TA with the data needed to generate the DPID. After authentication, the TA generates the DPID containing some identity information using the SM2 algorithm and then encrypts the DPID using the SM9 encryption algorithm to ensure that only the original TA can decrypt the broadcast information.

At registration, the VPK is generated by signing the DPID and other data using the SM2 encryption algorithm, and then the SM2 signature is broadcasted through the Trusted Data Center. After the receiver in the carpool network receives it, the enabling task loads the masked identity into the blockchain, which is decrypted using the SM9 decryption algorithm, and then further searches for the VPKT that is identified by the DPID, thus obtaining the user's VPK and the disseminated information.

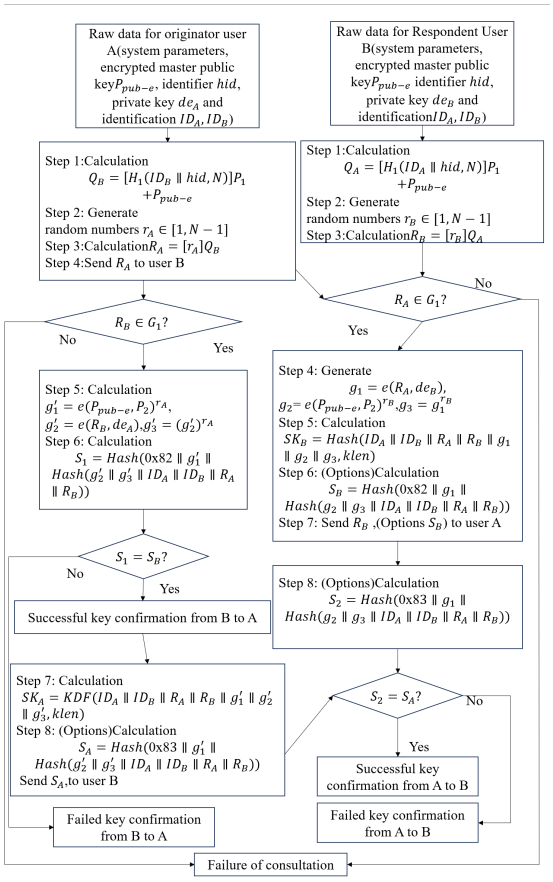

Figure 3. SM9 Key Exchange Protocol Flow.png.

After the cross-border TA obtains the user's DPID, the user makes a cross-domain request to the trusted data center, which verifies their identity through the A-Chain (B-Chain) of the application chain, obtains the DPID provided by the user by using the masked identity learned through broadcasting, searches for the VPKT corresponding to the DPID, and then verifies the signatures with the VPKs on the application chain, which has already ensured that the DPID provided by the user is the same as the VPKs registered in the original TA. The VPKT will then verify the user's identity with the VPK in the application chain to ensure that the DPID provided by the user is the same as that registered in the original TA, thus verifying the authenticity.

In this process, both parties have to carry out SM2 calculations on the user's cell phone and license plate numbers to generate the DPID; if the user provides the same cell phone and license plate numbers, then the DPID calculated by the two TAs is the same and can complete the verification to complete the authentication.

The digital signature in the SM2 algorithm is generated by a signer on the data, which, in the program, is the cross-border TA signing on the DPID, and then, the TA verifies the signature.

A flowchart of the SM2 algorithm is shown in Figure 5 [30], where IDA is the recognizable identity of subscriber A; M is the message to be signed, M' is the message to be verified, and G is a base point of the elliptic curve of prime order. SM2 uses part of the subscriber's identity private key for signing, and then, the public key is generated by the cross-border TA and sent for verification of signatures to complete the identity authentication.

Using the SM2 algorithm, on the one hand, can complete the authentication; on the other hand, it can use SM2

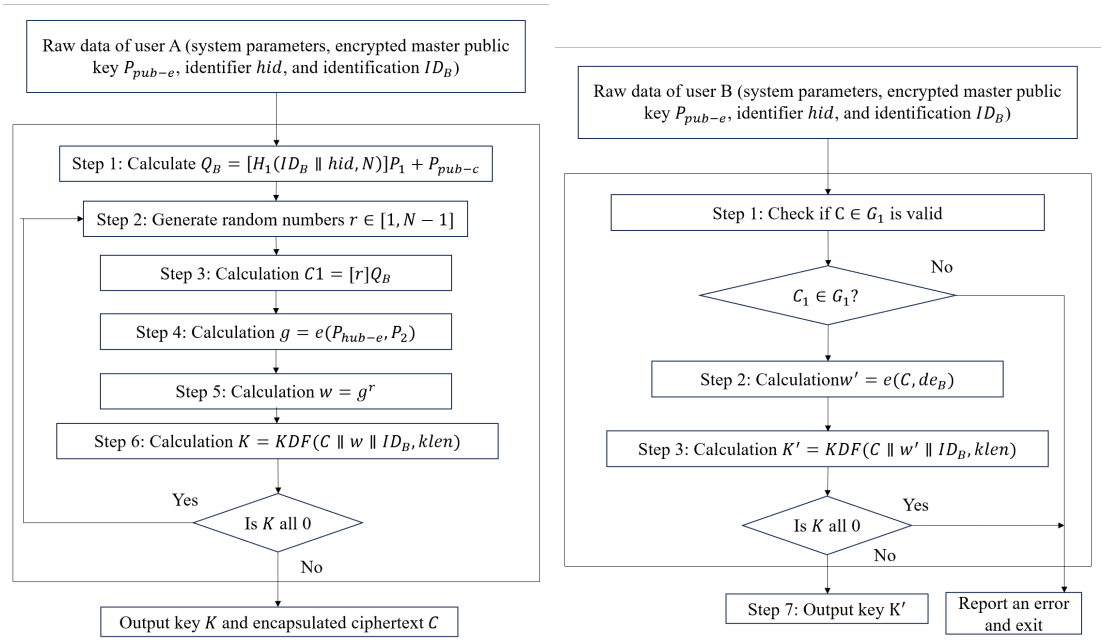

Figure 4. SM9 Key Encapsulation and Decapsulation Algorithm Flow.

to encrypt the user's DID and DPID and then upload them to the blockchain.

The cross-border user can only provide the same information during registration to get the same DPID in the cross-border TA to be transmitted back to the original TA. Only when the original TA receives the correct DPID can it complete the signature verification with VPK and then use the DPID to successfully decrypt the user's DID from the VPKT, thus strengthening the security of the data.

The application chain uses the cross-chain gateway to forward cross-chain requests and then conducts identity authentication audits through hash time locks and releases customs clearance certificates after the audits.

4. EXPERIMENTAL DESIGN

4.1. System architecture

The proposed system mainly implements the signature part of the NFT, the NFT generation on the application chain, and the verification time.

To implement NFT generation, you need to build and initialize the blockchain and complete operations such as uploading. To complete the experiment, it is necessary to design further the NFT related to the user to realize data uploading and recording time.

4.1.1. Blockchain creation

Creating a blockchain starts with choosing a blockchain platform; in the design of this project, the choice was made to deploy the private chain on the Ether platform. The Ether platform is an open-source blockchain platform that allows developers to build and deploy smart contracts and DApps. DApps are open-source applications based on the Ethereum blockchain, where a consensus is maintained between the user and programmer during the development process. The source code is available for examination, and the application is stored in the blockchain to ensure trust and transparency[31].

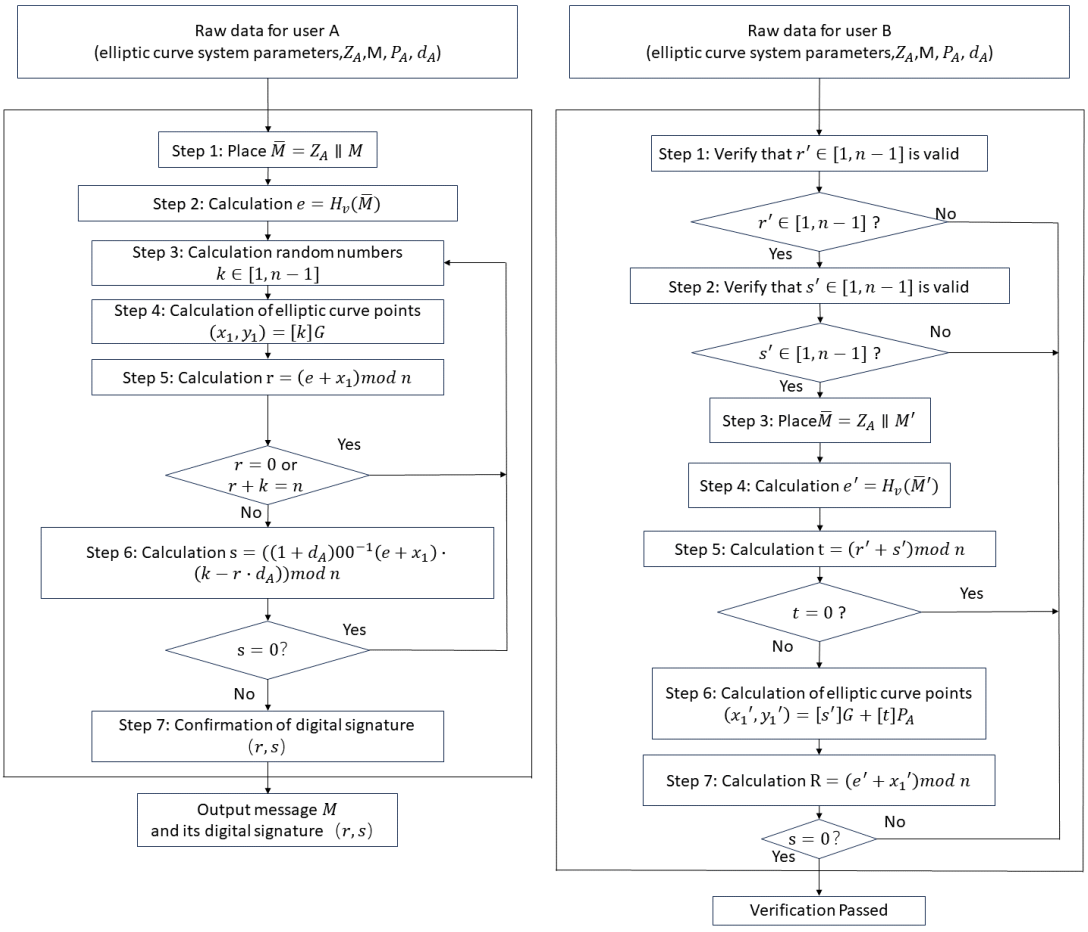

Figure 5. SM2 Digital Signature Generation and Digital Signature Verification Algorithm Flow.

The experiment used Windows 10, and Ganache was chosen to simulate the local Ethereum network. Ganache, a personal blockchain simulator and development environment for Ethereum and blockchain development, allows developers to quickly build a private Ethereum blockchain network in a local environment that contains one or more virtual nodes and generates virtual accounts for each virtual node, which can be used to simulate a real Ethereum account. Ganache provides a local and virtual blockchain for testing. It provides ten external user accounts, each assigned a unique Ethereum address and a private key associated with it. All the accounts come preloaded with 100 'fake' ethers [32].

After quickly creating an Ethereum network and accounts using Ganache, MetaMask is used to manage Ethereum and interact with Ethereum smart contracts. MetaMask is a widely used Ethereum wallet and browser plugin that allows users to create and manage Ethereum wallets, including operations such as generating public/private key pairs, backing up and restoring wallets, and providing a convenient interface for users to interact with Ethereum smart contracts. The interaction requires connecting MetaMask and Ganache, entering the RPC server address of the Ganache network in the MetaMask plugin, selecting an account from the Ganache interface, and entering Ether into MetaMask to complete the creation and preparation of the blockchain; after that, a written smart contract must be deployed into MetaMask.

4.1.2. Smart contract initialization

The writing and deployment of smart contracts is a key step in the development of blockchain applications. The requirements that need to be fulfilled for the project's smart contracts report are the need to complete the initialization, addition, and deletion of VPKTs in the smart contracts and the call to the NFT contract to complete the generation of NFTs for the data.

Truffle is used for innovative contract development, deployment, and testing. Truffle is a popular Ethereum innovative contract development framework designed to simplify and accelerate the process of developing, testing, and deploying Ethereum smart contracts. Truffle is scriptable, and extensive deployment and migration framework Mocha/Chai libraries are used for unit testing the smart contract functionalities[33]. It provides developers with tools and features that make building DApps and smart contracts easier.

Truffle was used to create a new project and check the correct structure before moving on to innovative contract development. Smart contracts need to complete the contents of the provided ABIs to call the VPKTA algorithm. This involves initializing, adding, deleting, and performing other operations on the VPKT within the smart contract. Similarly, these smart contracts complete the generation of the NFT and the subsequent data uploading process.

The ERC-721 standard contract implements the NFT function in the smart contract compilation. ERC-721 is a standard for displaying ownership of distinct NFTs. Moreover, it specifies an API for smart contract tokens[24].

For each NFT created, the smart contract records the generation and minting times of the tokens and triggers an information storage event. The user can call this function through the token ID to get the generation time, minting time, and minting execution time of the tokens.

4.1.3. Realization of NFT contract

Implementing the NFT contract is similar to the smart contract implementation described above and requires Truffle for compilation and deployment and generating an ABI for smart contract calls.

Truffle is used to compile the smart contract, deploy the compiled NFT smart contract after completion of compilation, transfer the smart contract to Ganache, and generate the contract's ABI and bytecode file for the previously mentioned smart contract to run and call.

The next step is to design the user interface for ease of use by creating a new HTML file and adding the required HTML structure and styles, including buttons, forms, text boxes, and other elements, to realize the interface for interaction with the smart contract. The smart contract functions are called through the ABI to realize the interaction with the blockchain.

For example, the user can fill in the NFT attributes in the interface and then trigger the create NFT function in the smart contract through the interaction button, interact with the smart contract deployed on the Ganache network through the front-end interface, and test the adding, deleting, and changing of the VPKT elements, as well as the NFT generating function to add new NFTs to the blockchain, which represents the TA in the project. The TA collects the user's identity information for encryption and then uplinks it to generate NFTs.

Web 3.0 is the incoming evolution of the World Wide Web (www). From its predecessor, people are now using the internet more than ever, not only for entertainment but for other purposes. In this iteration, decentralized networks are taking center stage, highlighting artificial intelligence (AI), blockchain, and other emerging technologies[34].

Web 3.0 represents an evolution of the centralized and siloed topology of Web 2.0 by focusing on more connected, decentralized, and open technology to democratize data and services between databases, tools, devices, people, teams, and organizations to provide secure single sources of truth on decentralized trust layers[35]. Interaction with smart contracts is achieved by writing web3.js API interfaces. The web3.js API was used to send the user's input to the Ethereum network after being received through a web interface[36].

After performing initialization, we load the Web 3.0 library and connect to the Ethernet network, get the current account, and store it in the component's state. Then, we create a contract instance using the ABI and address of the smart contract and store it in the component's state. The smart contract is called to get the data from the NFT and store it in the relevant variables. The blockchain is interacted with via the Web3 library blockchain, loading the smart contract data and providing an interface to cast and display the NFT.

4.2. Implementation

The experiments in the study focused on the time of NFT generation and validation. To verify these processes, the smart contract generated by the NFT of blockchain was deployed on a PC, and a time test was conducted to evaluate their duration. First, we need to determine the experimental parameters to be tested, considering the cost of the experiment and project requirements. We also need to assess the impact of experimental parameters, such as data upload speed and transaction cost, on NFT generation time.

To execute a smart contract, a user-controlled account must purchase a certain amount of gas using ether, the common currency in the Ethereum network. The gas cost is the transaction fee to encourage miners to include the code execution of the smart contract in the blockchain[37]. Thus, the purpose of the experiment was twofold: to test the time of NFT generation and to measure the consumption of generating an NFT.

We aimed to design and implement a basic Dapp with data uploading and display functions to measure the two parameters. The user interaction was realized through Web 3.0. Identical versions of Ganache, Truffle, and MetaMask were used on the same PC hardware. In addition to the generation of NFTs, the signature and verification of SM2 are also required, and the code implementation of SM2 and SM9 is in Python, which has excellent flexibility and operability. Considering that the federated blockchain has no impact on the model performance and is only used to maintain the blockchain, the federated blockchain was not activated in the experiments.

To accomplish the experimental generation of NFTs, we wrote two codes: the smart contract and the code for Web 3.0. First, we want the NFT to store the time spent minting itself, i.e., the signature information. A dynamic array is created for storing the tokens owned by the caller, a vibrant collection is designed for storing the generation time of the tokens, and the tokens held by the caller and the corresponding generation time are returned via a smart contract.

To measure the time required for NFT generation, several experiments are needed to obtain the average generation time and to minimize the effect of random factors on the results to ensure the reliability and stability of the results.

This is followed by collaborating with smart contracts through Web 3.0 to provide an interface on the web page that the user can interact with, giving input boxes and pop-ups to be used as data uploads and identity signatures and allowing the data to be visible in Web 3.0. From the above steps, we have realized a simple Dapp, compiled and deployed by Truffle on a virtual chain created by Ganache. Then, we ran it to realize the functions required to cast NFTs and display the time consumed.

Next, we cast NFTs for different data sizes using identical signatures and observed and recorded the time and

ether consumed for each NFT from the deployed web page and Metatask. For the accuracy of the data, five results were averaged for each test.

After testing, the total time for generating each 1024-bit NFT was approximately 6470 ms, and the consumed ether was 0.0309. Including the time for Metatask confirmation, the total consumed time for developing an NFT is approximately 10-15 s, basically in line with the IoV. As the data are only uplinked to the locally deployed blockchain, NFT casting is much faster than Ethernet, consuming only half the time to complete casting but significantly more ether. Comparable to other NFT generation schemes, it is quicker but consumes more.

5. DISCUSSION

Cross-domain authentication is mainly used in verifying NFT; in constructing a cross-border vehicle monitoring platform, it is necessary to comprehensively consider the cross-border data in different demand scenarios of data sharing modes and the whole life cycle of privacy protection.

The previous system model proposed the SM2 signature and signature verification method to complete the NFT authentication. At the same time, SM9 is used for cross-domain transmission of DPID, transforming the problem of cross-domain authentication into the realization of the SM2 algorithm of digital signature and signature verification.

Using the SM2 algorithm for signature verification can ensure the authenticity and validity of user identity. This design guarantees that all cross-border data are encrypted, which significantly improves the security and reliability of cross-border data interactions, prevents the occurrence of forged identity information, enhances the credibility of the whole system and data privacy protection, provides encrypted protection of cross-border vehicle user information, and reasonably manages the shared data to guarantee the user's data sovereignty and integrity.

The experiments conducted in this are rather crude and only intended to verify that the NFT's functionality can satisfy the model's needs. There is still much room for modification. This study did not improve the SM2 and SM9 algorithms because the main work was focused on the model design and experiments.

6. CONCLUSIONS

In this paper, we proposed a distributed identity management model for the NFT blockchain for cross-border data privacy protection. The model employs the NFT project scenario to avoid cross-border transfer of sensitive data using identity authentication to protect the privacy of cross-border users. It incorporates state secret SM2 and SM9 algorithms to complete key transmission and NFT verification, making it suitable for practical IoV applications. Future work will focus on the practical application of NFTs in identity authentication for IoV.

DECLARATIONS

Authors' contributions

Framework and algorithm design: Ying Z
Experimental design: Wang K

Availability of data and materials

Not applicable.

Financial support and sponsorship

This research is partially supported by NSFC-FDCT under its Joint Scientific Research Project Fund (Grant No. 0051/2022/AFJ), Macau, China.

Conflicts of interest

All authors declare that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

REFERENCES

1. Lu S, Ye J, Tan Y. Research on the security of data cross-border circulation in cyberspace. In: 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE); 2023. pp. 1–8. DOI
2. Casalini F, González JL. Trade and cross-border data flows. 2019:online ahead of print. DOI
3. Sun J, Liu D, Liu Y, Li C, Ma Y. Research on the characteristics and security risks of the internet of vehicles data. In: 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC); 2022. PP. 299–305. DOI
4. ehrani PM, Sabaruddin JSBH, Ramanathan DA. Cross border data transfer: complexity of adequate protection and its exceptions. *Comput Law Secur Rev* 2018;34:582-94. DOI
5. Shahriar Rahman M, Al Omar A, Bhuiyan MZA, Basu A, Kiyomoto S, Wang G. Accountable cross-border data sharing using blockchain under relaxed trust assumption. *IEEE Trans Eng Manage* 2020;67:1476-86. DOI
6. Islam MR, Rashid MM. A survey on blockchain security and its impact analysis. In: 2023 9th International Conference on Computer and Communication Engineering (ICCCE);2023. pp. 317–21. DOI
7. Zhang J. The influence of blockchain technology on cross-border e-commerce and its governance path. In: 2022 6th Annual International Conference on Data Science and Business Analytics (ICDSBA); 2022. pp. 14–8. DOI
8. Wang Q, Li R, Wang Q, Chen S. Non-fungible token (nft): overview, evaluation, opportunities and challenges. *arXiv* 2021:2105.07447. hrefhttps://doi.org/10.48550/arXiv.2105.07447DOI
9. Hong G , Chang H. A study on corporate information assets management system using nft. In: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC); 2022. pp. 608-10. DOI
10. Saifullah SI, Islam M, Ferdous MS, Chowdhury F. Non-fungible token (nft): Analyzing marketplaces and non-user perspectives. In: 2022 25th International Conference on Computer and Information Technology (ICCIT); 2022. pp. 1044–51. DOI
11. Gao S, Peng Z, Tan F, Zheng Y, Xiao B. Symmeproof: compact zero-knowledge argument for blockchain confidential transactions. *IEEE Trans Dependable and Secure Comput* 2023;20:2289–2301. hrefhttps://doi.org/10.1109/TDSC.2022.3179913DOI
12. Mohan PM, Balachandran V, Quan OZ, Xin JPZ, Divakaran DM. Nft-merit: An nft-based module credit management system on ethereum blockchain. In: 2022 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE); 2022. pp. 472–6. hrefhttps://doi.org/10.1109/TALE54877.2022.00083DOI
13. Tharun T, Vamshi A, Eswari R. Nft application for music industry using blockchain smart contracts. In: 2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT); 2023. pp.1–6. DOI
14. Takahashi H, Lakhani U. Sustainable nft blockchain storage for high availability and security. In: 2022 IEEE 11th Global Conference on Consumer Electronics (GCCE); 2022. pp. 264–7. DOI
15. Chen Y, Wang Z, Liu X, Wei X. A new nft model to enhance copyright traceability of the off-chain data. In: 2022 International Conference on Culture-Oriented Science and Technology (CoST); 2022. pp. 157–62. DOI
16. Manzoor K, Noor U, Rashid Z. Nft-based blockchain-oriented security framework for metaverse applications. *arXiv* 2023;2307:10342. DOI
17. Bellagarda J, Abu-mahfouz AM. Connect2nft: a web-based, blockchain enabled nft application with the aim of reducing fraud and ensuring authenticated social, non-human verified digital identity. *Mathematics* 2022;10:3934. DOI
18. Sun N, Zhang Y, Liu Y. A universal privacy-preserving multi-blockchain aggregated identity scheme. *Appl Sci* 2023;13:3806. DOI
19. Wang Q, Yu G, Fu S, Chen S, Yu J, Xu X. A referable nft scheme. In: 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2023. pp. 1–6. DOI
20. Khalil U, Malik OA, Hong OW, Uddin M. Dscot: an nft-based blockchain architecture for the authentication of iot-enabled smart devices in smart cities. *arXiv* 2022:2211.04803. DOI

21. Neisse R, Hernández-Ramos JL, Matheu-García SN, et al. An interledger blockchain platform for cross-border management of cybersecurity information. *IEEE Internet Comput* 2020;24:19–29. DOI
22. Peng Z, Xu J, Hu H, Chen L. Blockshare: a blockchain empowered system for privacy-preserving verifiable data sharing. *IEEE Data Eng Bull* 2022;45:14–24. Available from: https://api.semanticscholar.org/CorpusID:251667807. [Last accessed on 29 Nov 2023]
23. Dang TLN, Nguyen MS. An approach to data privacy in smart home using blockchain technology. In: 2018 International Conference on Advanced Computing and Applications (ACOMP); 2018. pp. 58–64. DOI
24. Konagari A, Kusuma HP, Chetharasi S, Kuchipudi R, Babu PR, and Murthy TS. Nft marketplace for blockchain based digital assets using erc-721 token standard. In: 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS); 2023. pp. 1394–8. DOI
25. Sujeetha R, Deiva Preetha CAS. A literature survey on smart contract testing and analysis for smart contract based blockchain application development. In: 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC); 2021. pp. 378–85. DOI
26. Wang M, Long Y. Sm9 digital signature with non-repudiation. In: 2020 16th International Conference on Computational Intelligence and Security (CIS); 2020. pp. 356–61. DOI
27. Tian C, Wang L, Li M. Design and implementation of sm9 identity based cryptograph algorithm. In: 2020 International Conference on Computer Network, Electronic and Automation (ICCNEA); 2020. pp. 96–100. DOI
28. Liu P, Ye NQ, Han HX, et al. Power data collection terminal protection based on sm9. In: 2021 International Conference on Power System Technology (POWERCON); 2021. pp. 1877–82. DOI
29. Gb/t 38635.2-2020, information security technology–identity-based cryptographic algorithms sm9-part 2: algorithms. *Standardization Administration of China*; 2020. Available from: https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=02A8E87248BD500747D2CD484C034EB0. [Last accessed on 29 Nov 2023]
30. Gm/t 0003-2012, public key cryptographic algorithm sm2 based on elliptic curves—part 1: general. *Standardization Administration of China*; 2016. Available from: https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=3EE2FD47B962578070541ED468497C5B. [Last accessed on 29 Nov 2023]
31. Sayeed S, Marco-gisbert H, Caira T. Smart contract: attacks and protections. *IEEE Access* 2020;8:24416-27. DOI
32. Patidar K, Jain S. Decentralized e-voting portal using blockchain. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT); 2019. pp. 1–4. DOI
33. Maya P, Salam PA. Implementation of a blockchain based dapp for p2p electricity trading. In: 2023 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE); 2023. pp. 1–6. DOI
34. Sy MPM, Marasigan RI, Festijo ED. Hyperledger-operated blockchain integration: writing, deploying and testing custom chaincode. In: 2023 Sixth International Symposium on Computer, Consumer and Control (IS3C); 2023. pp. 151–4. DOI
35. Borgen KAT. Web3 for sensitive data, enterprise, government, private, and permissioned use. In: 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain); 2022. pp.1–6. DOI
36. Dhanvardini R, Martina P, Vijay R, Amirtharajan R, Pravinkumar P. Development and integration of dapp with blockchain smart contract truffle framework for user interactive applications. In: 2023 International Conference on Computer Communication and Informatics (ICCCI); 2023. pp. 1–6. DOI
37. Wu S, Chen Y, Wang Q, Li M, Wang C, Luo X. Cream: A smart contract enabled collusion-resistant e-auction. *IEEE Trans Inform Forensic Secur* 2019;14:1687-701. DOI