Article | Received 7 March 2024; Accepted 30 April 2024; Published 20 May 2024
https://doi.org/10.55092/blockchain20240003

Blockchain-enabled cross-border insurance: from legal issues, solution design, to implementation

Jiaxin Ran[1,†], Dechuan Li[1,†], Qixin Zheng[2], Jerome Yen[1], and Yingjie Xue[3,*]

[1]Faculty of Science and Technology, University of Macau, Macao, China
[2]Faculty of Law, University of Macau, Macao, China
[3]Thrust of Financial Technology, Society Hub, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou, China

†Co-first Author

* Correspondence author; E-mail: yingjiexue@hkust-gz.edu.cn.

Abstract: Traditional insurance contracts are beset with challenges such as cumbersome notification, complex underwriting and inefficient claims settlement, all of which impede the industry's growth. In response, the digital transformation of insurance companies has become essential. Blockchain technology, with its inherent features of transparency and immutability, offers significant potential for transforming the insurance industry and there has been considerable research on using blockchain technology in the insurance sector. However, when it comes to cross-border insurance service, current solutions fall short in effectively navigating the legal and compliance complexities inherent in cross-border insurance service delivery. When transmitting data across borders, it is essential to adhere to the legal requirements of cross-border laws and regulations, especially considering the variations in regional data protection and privacy legislation. A general solution for managing cross-border data transfer that both supports service delivery and adheres to compliance standards, has yet to be developed. In this paper, we propose solutions to secure data transfer in cross-border insurance service provision. First, we examine the legal and compliance challenges associated with cross-border data transfer. Following this, we introduce a system that integrates blockchain, smart contracts, and Trusted Execution Environment (TEE) to enhance cross-border insurance services. We propose a cross-chain protocol, which incorporates hash-locking and the notary mechanism for efficiency and security. We develop a prototype for implementing our proposed protocol and conduct extensive testing to show the practicality and security of our proposed protocol.

Keywords: cross-border insurance; blockchain; cross-chain; TEE; data security

1. Introduction

The integration of global financial markets has fueled a boom in cross-border business in various economic and financial sectors in the past few years. It is noteworthy that Focarelli and Pozzolo [1], Van der Zwet [2], and Schoenmaker and Sass [3] have identified the insurance sector as being significantly more internationally oriented compared to the banking sector. Take Europe as an example, Schoenmaker and Sass [3] observe a statistically significant increase in cross-border insurance activities among the 25 largest European insurers. Turning our attention to Asia, particularly since the inception of China's Guangdong-Hong Kong-Macau Greater Bay Area in 2017, there has been a notable development in financial market integration. The cumulative volume of cross-border RMB settlements within the

Greater Bay Area has surpassed 21 trillion, indicating a deepening of financial market connectivity [4]. Insurance companies have progressively introduced a variety of cross-border insurance products, including cross-border health and auto insurance. Consequently, the evolution of a globally regionalized economy has created a substantial market for cross-border insurance services. This development has, consequently, led to a significant increase in focused research in this field.

In the context of cross-border insurance business, the transfer and authentication of data across borders are constrained by legal and trust-related challenges. Consider the case of cross-border health insurance. On the one hand, when insured individuals directly submit claims data, there exists a motivation to furnish falsified information in an attempt to defraud the insurance company for a larger settlement. On the other hand, if hospitals are responsible for providing claims-related data to insurance companies, there is a risk of collusion where hospitals might leak patient data for profit, thereby compromising the protection of patients' data privacy. John Jiang and Ge Bai discover that 53% of breaches involving protected health information are internal [5]. For example, in 2021, the prominent US-based internet company Facebook admitted to a substantial data breach, which resulted in the compromise of personal information belonging to over 533 million users [6]. What's worse, pinpointing responsibility for data breaches is challenging due to the untraceable nature of data transfer between hospitals and insurance companies. In cross-border contexts, the legal liability for data leakage becomes even more complex to ascertain due to varying laws across different regions.

Blockchain technology, a paradigm-shifting innovation in digital record-keeping, holds promise in addressing these issues due to its unique attributes of decentralization, transparency, and security [7]. The inception of blockchain technology is inextricably linked to the creation of Bitcoin by an individual or group under the pseudonym Satoshi Nakamoto [8]. A significant advancement in this technology is represented by smart contracts, which are self-executing contracts with the terms of the agreement directly embedded in the code. The blockchain technology provides secure, reliable, and transparent data storage and transfer, facilitated by the joint efforts of numerous network nodes. The advent of smart contracts, executable programs on the blockchain, has opened avenues for automating insurance services through code. Furthermore, blockchain allows entities without mutual trust to engage in value exchanges and interactions, eliminating the need for a trusted intermediary [9]. All of these features showcase the technology's versatility and applicability in the insurance industry.

However, current blockchain solutions typically manage all data within a single blockchain [10, 11]. Given the legal constraints across different regions, relying on a single blockchain to facilitate data transfer and authentication in cross-border insurance scenarios is impractical. To overcome the challenges of value transfer and data communication among different blockchains, which often exhibit a high degree of heterogeneity [12], various cross-chain technologies have been developed. Currently, several researchers have classified cross-chain technologies into four categories [12–14]: notary mechanisms [15], hash-locking [16], sidechains [17], and distributed private key control [13]. Despite these advancements, the widespread adoption of cross-chain technology is limited due to ongoing issues related to compatibility, security, and efficiency [18].

Trusted Execution Environment (TEE) is gaining prominence for its security capabilities, which are rooted in hardware isolation. TEE establishes a secure area within the central processor, where sensitive data can be securely stored and processed. Consequently, TEE can serve as a robust foundation, enhancing the overall security of systems that integrate blockchain and cross-chain technologies.

In this paper, to address the challenges in cross-border insurance, we propose a cross-chain protocol that combines the notary mechanism with hash-locking. Building upon this protocol, we develop a cross-border data transfer system which uses TEE as a security foundation, to address the specific security requirements of cross-border insurance business scenarios. The

key contributions of our paper are summarized as follows:

(1) We design a cross-chain protocol by integrating the notary mechanism with hash-locking. This approach facilitates the process of cross-chain data transfer while simultaneously bolstering its security.

(2) We present a TEE-based cross-chain system designed to support data transfer and authentication in cross-border insurance operations securely. This system offers a secure and compliant solution tailored to the unique needs of cross-border insurance.

(3) We implement the proposed cross-chain system, facilitating data transfer between two consortium blockchains independent of their consensus mechanisms. Experimental evaluations demonstrate that our system exhibits good processing speed and low latency.

The rest of the paper is organized as follows: Section 2 introduces the security requirements of cross-border business and outlines our motivation. Section 3 presents the related work. In Section 4, we discuss the legal issues associated with cross-border data transfer. Section 5 offers a high-level overview of the system architecture. Section 6 details the specific design of our system and elucidates the operational process through a practical use case. Section 7 showcases the user interface, validates the system's feasibility, and conducts a security analysis of the proposed system. Finally, Section 8 concludes our work, providing directions for future research and potential developments in this field.

2. Motivation and security requirements

The motivation for employing cross-chain architecture instead of a single blockchain to achieve cross-border data transfer lies in two points. On the one hand, the jurisdiction over data on the blockchain is a question and it is unrealistic for different countries to jointly maintain one blockchain to record and transfer the insurance data, since it involves national information security issues.

On the other hand, different laws across various countries may lead to disputes over the management of data storage. For example, GDPR gives the specific secure requirement of data erasure. According to Article 17 in GDPR, individuals have the right to have their personal data erased under certain circumstances, such as when the data is no longer necessary for the purpose it was originally collected or processed for, and the processors must erase these data in time. However, the Data Security Law in China lacks the corresponding legal provisions. If we use a single-chain architecture, it is difficult to define the right to erase data should follow whether the regulations outlined in GDPR, or those in Data Security Law of China.

Moreover, given that the cross-border data transfer in the insurance business scenarios involves a lot of sensitive data, more attention needs to be paid to legal compliance in cross-border insurance. Thus, we use cross-chain rather than a single blockchain to facilitate data transfer and authentication in cross-border insurance scenarios in this paper.

Data transfer in cross-border business scenarios must address the following security needs:

• **Confidentiality.** All parties involved in cross-border insurance business scenarios have the incentives to leak private data. For example, the insurance companies sell the insured person's private data to illegal organizations for profit. Therefore, achieving data confidentiality is crucial, meaning that data should not be exposed to any party without consent.

• **Immutability.** Existing cross-border data transfer processes are often recorded in the form of paper documents or electronically, which can be easily tampered with and may lead to serious data leakage incidents. It is essential to establish a process for data transfer and storage that is tamper-proof.

• **Traceability.** Liability for data breaches in cross-border insurance is generally difficult to determine accurately because of the many procedures involved and the different laws in different regions. Therefore, we need to make the cross-border data transfer process traceable to provide assistance in determining legal liability in data leakage incidents.

• **Security and operability trade-offs.** In general, increasing operational complexity and

difficulty will enhance system security. However, if the system is too difficult to operate, it will increase the cost or even be difficult to realize in industry. So we need to strike a balance between system security and operability.

3. Related work

3.1. Legal issues and compliance

In the context of global innovation and digital development, the development of cross-border insurance business is accompanied by an increased demand for cross-border data transfer. The cross-border transfer of data is fraught with various risks and challenges, including different regulations across countries and the potential for data tampering or leakage during transfer. Current research in this domain primarily focuses on analyzing the sensitivity of data and identifying the security risks it entails [19]. It also explores effective strategies for risk prevention and control, aiming to facilitate the open use of data and unlock its value [20]. Research concerning the regulation of cross-border data transfer mainly address the issues in applying outbound data rules and standard contracts. Solutions are being proposed from both international and domestic legal perspectives to address these challenges [21]. Comparing the data regulatory approaches of the US and the EU is highly instructive, offering valuable insights into their advanced practices [22]. The academic community is increasingly advocating for regulations on cross-border data transfer to be context-specific and to employ categorized management. Despite this, there remains a gap in existing research, particularly in detailed discussions on the regulation of cross-border data transfer in specific scenarios. There is an urgent need to strengthen research on the regulation of cross-border transfer of data.

We should promote the development of the cross-border insurance industry based on preventing and reducing legal compliance risks associated with the cross-border transfer of data. This entails achieving the right balance between the dual goals of 'Risk Control' and 'Industry Development'. At the same time, we can apply relevant technology to enhance compliance capabilities. Compliance technology not only enables insurance companies to save substantial costs but also effectively identifies risks and provides solutions [23]. Strengthening the application of data technology and compliance technology can systematically enhance the technological support capabilities for the security of cross-border insurance data transfer in China, efficiently implementing the requirements of outbound data regulations [24].

3.2. Blockchain in insurance industry

Blockchain inherently carries a 'trust gene', thanks to its cryptographic algorithms and timestamp technology, making it naturally suited for fostering trust. There are many distrust issues in insurance business scenarios. For example, parties involved in insurance may leak the private data for profit, and insurance companies may delay or even refuse to settle claims by not acknowledging receipt of data. The application of blockchain to the insurance industry can effectively mitigate these distrust issues. Specifically, leveraging smart contracts to automatically execute the data transfer process could reduce manual involvement and mitigate the risk of data breaches. Even if a data breach occurs, the fully recorded data transfer process on the blockchain enables easy identification of the cause of the breach. Additionally, the data transfer process becomes traceable and tamper-proof by utilizing blockchain technology. Therefore, if the insurance company denies the claim after receiving the data, the insured person could use the data transfer records on the blockchain as evidence to sue the insurance company.

Multiple researchers [25–27] have highlighted the potential applications of blockchain in the insurance sector, noting its ability not only to enhance productivity but also to foster the creation of new services and products. Blockchain's versatility allows it to be utilized in various aspects of the insurance industry. To be specific, as for insurance data storage, Zhou

et al. [28] propose a blockchain-based medical insurance storage system, MIStore, to provide a high-credibility to users. This system utilizes blockchain technology to provide a secure solution for storing sensitive data in insurance. In terms of insurance processes, Mayank Raikwar *et al.* [10] propose a blockchain-based framework to support insurance transaction execution, which gives a solution to automate and speed up insurance process. Nizamuddin and Abugabah [29] present an auto-insurance framework based on blockchain to regulate the automobile insurance process and automate payments to avoid errors caused by manual claims. In the area of insurance fraud risk management, Liu *et al.* [30] and Saldamli *et al.* [31] propose a blockchain based solution for health insurance fraud detection to prevent insurance fraud. Zhang *et al.* [32] utilize blockchain and BERT-LE model to identify fraud in medical insurance accurately and improve the efficiency.

While applying blockchain to the insurance sector, regulatory issues cannot be ignored. Richard Brophy [33] offers an operational and regulatory review of blockchain applications in insurance. The author points out that insurance is a heavily regulated industry so laws and regulatory approaches could impact on blockchain applications in the insurance sector.

3.3. Cross-chain technology

Cross-chain technology emerged as a solution to the 'value isolation' issue in blockchain, a problem stemming from the significant heterogeneity between different blockchain systems. Generally, cross-chain technologies can be classified into four main categories: hash-locking, notary mechanisms, sidechain/relay chain, and distributed private key control [34–37]. This classification reflects the diverse approaches developed to facilitate interoperability and value transfer across distinct blockchain networks.

Sidechain technology [17] employs a two-way peg mechanism to facilitate the transfer of crypto assets between the main chain and the sidechain at a predetermined exchange rate. The sidechain functions as an independent secondary blockchain with its own set of rules and configurations. When assets from the main chain are transferred to a sidechain, the corresponding assets on the main chain are locked, remaining so until they are transferred back to the main chain [38].

Another pivotal advancement in cross-chain technology was made by Ripple Labs in 2015. They introduced the InterLedger protocol [39] addressing the challenges of interaction between different blockchain systems. This protocol laid the groundwork for what would eventually evolve into the notary mechanism. In the notary mechanism, the asset transfer is coordinated by a set of notaries, and each transfer is organized into groups without a set of globally available notaries [15].

The use of hash-locking was first explored in the Bitcoin Lightning Network in 2015 [16]. They provide a comprehensive explanation of how the Lightning Network operates, centering around two key concepts: RSMC (Recoverable Sequence Maturity Contract) and HTLC (Hashed Timelock Contract). These mechanisms are pivotal in ensuring the security and reliability of payments, as well as enhancing the transaction efficiency of the Bitcoin system.

Distributed private key control adopts distributed nodes to control the private keys of various assets in the blockchain system, separating the right to use and ownership of the assets [40]. This enables the control of the assets on the chain to be securely transferred to a decentralized system, and at the same time mapping the assets on the original chain to the other chain to realize the transfer of value between different blockchain systems. The operations that enable and disable distributed control rights management are called: lock-in and lock-out. Lock-in is the process of achieving control over an asset and asset mapping and lock-out is the reverse operation of lock-in, returning control of the asset to the owner. Distributed private key technology uses multiple distributed private key generators (PKGs) to relieve the key escrow problem and decentralize the power on the authority [41]. Representative projects that utilize distributed key control include Wanchain [42] and Fusion [13].

Deng *et al.* [37] compare four cross-chain technologies such as hash-locking, notary mechanism, sidechain/relay chain and distributed private key control and proposed a hash-locking mechanism utilizing sidechain as a third-party trading platform in 2018. Dai *et al.* [43] propose a hash-locking cross-chain transaction mechanism using notary mechanism to simplify the transaction process, and introduce the Diffie-Hellman algorithm for the key negotiation to strengthen the security in 2020. Sun *et al.* [44] combine a notary scheme and hash-locking with the introduction of rewards and penalties in 2022. Han *et al.* [45] propose a standardized five-layer blockchain architecture which includes network layer, data layer, consensus layer, incentive layer and application layer. Blockchain interoperability can be not entirely dependent on this architecture, as some cross-chain technologies can serve the purpose of cross-layer. The author also categorizes the purpose of cross-chain into four categories, namely asset transfer, asset exchange, data sharing and cross-chain smart contract execution.

3.4. Trusted Execution Environment (TEE)

Trusted Execution Environment (TEE) is gradually coming into the public's view since it meets the increasing demands for data security and privacy protection. GlobalPlatform, an authoritative international standards organization, gave a specific definition of TEE in 2010: Trusted Execution Environment is an environment which runs alongside a rich operating system and provides security services to that rich environment [46]. Specifically, TEE is a hardware-assisted security architecture that builds a secure area in the central processor and the sensitive data is stored and computed in this secure area. Secure execution, openness and trust are its main parts [47]. TEE has attracted many researchers from academia and industry because it provides the following security properties [47–50]:

• *Secure boot.* Secure boot loads immutable and verified images to an enclave when the host starts and this ensures a chain of trust among the enclave images, operating system components, and configurations, which means only code of certain properties can be loaded.

• *In-enclave execution.* Sensitive data and code are stored and executed in a physically isolated area in the central processor, thus the data and code are protected against eavesdropping and tampering by the outside world.

• *Remote attestation.* TEE can provide remote attestation to prove its trustworthiness for the third-party and verify the code and data running in TEE are correct.

• *Sealing.* Sealing binds the data to a specific enclave's state by a unique key or a platform key. Sealing data ensures TEE securely persist and retrieve the enclave data so that can be in line with application requirements under circumstances such as system reboot, power interrupt and so on.

• *Isolated peripherals.* Secure peripheral sharing and trusted I/O path protects the authenticity and confidentiality of communication between TEE and peripherals.

TEE can be combined with blockchain in a complementary way to provide solutions to efficiency and security issues that affect the widespread use of blockchain [51]. Milutinovic *et al.* [52] and Zhang *et al.* [53] employ TEEs in existing consensus schemes to reduce energy consumption and to improve time efficiency. Li *et al.* [54] integrate TEE with PoS protocol to overcome existing its security shortcomings such as the nothing at stake attack [55] and long-range attack [56]. Besides, multiple researchers [57–59] attempt to combine smart contracts with TEE to ensure the confidentiality for the execution and storage of smart contracts.

TEE also plays an important role in improving the security and efficiency of cross-chain mechanisms. Bentov *et al.* [60] leverage TEE to support real-time cross-chain cryptocurrency trades and secure tokenization of assets pegged to cryptocurrencies. Lan *et al.* [61] encrypt cross-chain communication data on the relay chain with the assistance of TEE to enable confidential interoperability across blockchains.

4. Legal issue

Various countries possess diverse data protection regulations. For instance, in the European Union, the General Data Protection Regulation (GDPR) [62] constitutes a privacy statute enacted in May 2018. It aims to protect the personal data of European Union residents through the imposition of obligations on entities engaged in the collection, processing, and storage of personal data. Similarly, the United States adheres to the Health Insurance Portability and Accountability Act (HIPAA) [63] , while China enforces the Personal Information Protection Law (PIPL) [64] . The Asia-Pacific Economic Cooperation (APEC) has instituted the Cross-Border Privacy Rules (CBPR) system [65], which is a voluntary, multilateral framework that aims to facilitate cross-border data flows while protecting personal information. It requires participating nations to implement fundamental privacy protections and institute a system for enforcement and dispute resolution. The comparison of legislation on cross-border data security in different countries or regions is summarized in Table 1.

Table 1. Legislation on cross-border data security in different countries or regions.

Countries or Regions	Legislation	Data Definitions	Safeguards for Data Processing and Transfer	Cross-border Data Transfer
Mainland of P.R.C.	Cybersecurity Law, Data Security Law	Cybersecurity Law: Article 76(4),76(5); Data Security Law: Article 3	Cybersecurity Law: Article 37; Data Security Law: Article 3	Cybersecurity Law: Article 37
EU	GDPR	Article 4(1): Definitions of 'personal data'	Article 4(2): Definitions of 'processing'; Article 5: Principles relating to processing of personal data	Article 4(23): Definitions of 'cross-border processing'; Chapter V: Transfer of personal data to third countries or international organisations.
U.S.	The CLOUD Act, Clarifying Lawful Overseas Use of Data Act [66]	SEC.102(1): electronic data held by communications-service providers	SEC.103: Preservation of records; Comity analysis of legal process.	Second part of the CLOUD Act: CSPs subject to U.S. jurisdiction must disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data. [67]
Hong Kong	Personal Data (Privacy) Ordinance [68]	Article 2(1): Interpretation of 'personal data'	Article 2(1): Interpretation of 'processing'	Part 6: Matching Procedures and Transfer of Personal Data, etc.; Article 33: Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances.
Singapore	The Personal Data Protection Act (PDPA) [69]	Article 2(1): Interpretation of 'personal data' Article 3: Purpose	Article 2(1): Interpretation of 'processing' Article 24: Protection of personal data	Article 26: Transfer of personal data outside Singapore.

Pertinent legal provisions in China establish a foundation for refining regulations governing cross-border data flow. China has instituted a system for personal information and data protection with the framework of the Cybersecurity Law [70], the Data Security Law [71] and the Personal Information Protection Law [64] . These regulations mentioned above provide a legal framework for the processing and cross-border transfer of personal information and data. They also establish fundamental institutional guarantees for cybersecurity, data security, and the protection of personal information rights and interests in the digital era. China has successively issued a series of administration exposure drafts represented by the Administration

of Network Data Security (Exposure Draft) [72] . The Measures for the Security Assessment of Outbound Data Transfer [73] issued by the Cyberspace Administration of China has come into force on September 1, 2022. These measures emphasize that data processors should regulate outbound data transfer activities and apply to the security assessment of the outbound data transfer. The aforementioned regulations, the administration exposure draft and the relevant standards and guidelines collectively represent China's in-depth legislative exploration of cross-border transfer of personal information and data. Although China's existing laws and regulations already provide principled provisions, they have yet to establish corresponding mandatory norms or recommended standards for the outbound transfer of data in cross-border insurance scenario, and the cross-border transfer of these data faces numerous risks and challenges as a result.

Take cross-border health insurance as an example. In cross-border health insurance scenarios, personal medical data often needs to be transferred across borders. Although specific standards for the cross-border transfer of personal medical data are limited, the "Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information" issued by International Organization for standardization (ISO) in 2004 mentions that personal medical data should not be transferred except for the transfer necessary to protect the vital interests of data subjects, unless the explicit consent of the data subject is obtained. Both Chinese and foreign standards for the protection of personal health data underscore the requirement to obtain express or explicit consent from the data subject before the data collection.

Major digital economies, including the United States and the European Union, have enacted corresponding regulations for cross-border data transfer from an 'industry promotion' standpoint. For instance, in terms of personal information protection and data security, the United States has consistently advocated for extensive freedom in data processing and promoting the aggregation of data to the United States, emphasizing the free flow of data and maximizing the value of data. Notably, specific restrictions on outbound personal medical data transfer activities have not been implemented.

Under the General Data Protection Regulation (GDPR), organizations generally need to obtain the consumer's consent before transferring their data across borders. Various mechanisms exist for transferring data under GDPR, one of which is obtaining explicit consent from the data subject (the consumer). Consent should be freely given, specific, informed and unambiguous. According to Article 49 of GDPR, "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards." In the specific practices of EU countries, industry organizations in some nations publish templates for the use of personal data in the form of guidance documents. For example, the Insurance Industry Association in the United Kingdom issued The Data Protection Insurance Market Core Uses Information Notice in 2018 [74], recommending that enterprises either refer to the document in practice or directly link to the document in their privacy policy. Such industry guidance documents are pertinent and instructive for personal information protection within their respective sectors. For cross-border transfer of personal information related to cross-border insurance, China regards 'inform + consent' as a necessity rather than an optional exemption. "Where a personal information processor provides personal information for any party outside the territory of the People's Republic of China, the processor shall inform the individuals of the overseas recipient's name and contact information, the purposes and means of processing, the categories of personal information to be processed, as well as the methods and procedures for individuals' exercise of the rights provided in this Law over the overseas recipient, etc., and shall obtain individuals' separate consent." [75]

In the context of the strategic value of data, the cross-border flow of data in insurance scenario involves not only the security of personal data or the effective use of commercial

data, but also issues of 'national security' and 'international political games'. In addition to the national regulatory authorities optimizing the regulatory measures from the perspective of outbound data transfer activities, the safe and orderly development of cross-border insurance data flow also requires the country to promote the establishment of international data cross-border flow of mutual trust mechanism. However, China has yet to establish cooperation channels for cross-border data flow with major digital economies such as the EU and the US. For the EU, China is not one of the countries that it has identified as meeting the requirement of 'appropriate safeguards' in terms of data security, resulting the lack of regulatory mechanism for cross-border data flow between the EU and China at present [76]. The data transfer across different countries is of great significance to promote scientific research and industrial development in related fields and elevating the quality of services. However, an increasing number of countries or regions are advocating for the data localization laws concerning 'important' and 'sensitive' data due to national security or personal privacy protection. This is not conducive to promoting the free flow of data, let alone the progress of scientific research and industry development. Most countries have data sovereignty laws that require specific types of data to be stored and processed within their borders. Some of these countries include Canada, California (United States), European Union (GDPR), Germany, France and Australia. Other countries with strict data localization laws include Brunei, China, Indonesia, Nigeria, Russia and Vietnam. These laws can create challenges for data transfer in cross-border insurance scenario, as the insured, data providers and insurance companies must comply with the data sovereignty requirements of each country.

5. System overview

5.1. Assumptions

Assumption 1: *The TEE hardware is correctly implemented and securely manufactured.* Recent research [49–51, 77] has shown that TEE may suffer from side-channel attacks. In other words, the attacker may observe the shared resources to obtain the control flow and the data access mode of the enclave program to infer the sensitive information in the enclave. However, side-channel attacks are relatively difficult to be exploited and most of the existing security and encryption techniques are generally facing the risk of side-channel attacks. As a result, we do not consider the side-channel attacks for TEE in this paper. Besides, we trust the TEE hardware and we assume that the TEE hardware is correctly implemented and securely manufactured.

Assumption 2: *The blockchain system is trustable and available all the time.* The design and implementation of our system does not rely on any underlying blockchain consensus algorithm. We assume that the blockchains perform the required calculations correctly all the time and we do not consider communication breakdowns, that is, users can always send requests to the blockchain network and get responses.

Assumption 3: *The system we designed is legally compliant.* As discussed in Section 4, some countries and regions have well-established cross-border data transfer laws, while others lack relevant legal provisions. Therefore, we mainly refer to GDPR when design the data transfer system in cross-border insurance business as it is a relatively complete provision for cross-border data transfer. Our system complies with the requirements for cross-border data transfer in GDPR, and therefore, we assume that the system we designed is legally compliant.

5.2. High level architecture

Considering the technical selection discussion in Section 6.2 & Section 6.3 & Section 6.4 (which will be elaborated in the next section), we combine cross-chain technology with

TEE to propose a cross-border insurance data transfer system. This system is designed to provide security and legal compliance solution for the data transfer process in cross-border insurance business.

The data transfer in cross-border insurance business starts with the insured person authorizing the data provider to provide data to the insurance company. After successful authorization, the insured person is no longer involved in the subsequent data transfer process to ensure the correctness of the data. We utilize TEE for key escrow, random number generation, and data detection before uploading to improve the security of the whole system. On the other hand, we utilize cross-chain technology to enable cross-border data transfer in cross-border insurance business scenario to meet the security requirements of confidentiality, traceability and immutability in the data transfer process.

The high-level architecture, depicted in Figure 1, consists of three layers in our cross-border insurance data transfer system: the data layer, system layer, and application layer.

Data layer This layer provides a secure base for the entire system. The Data layer mainly provides three functions:

- *Privacy detection before uploading.* Before the data is uploaded to the chain, data detection is performed to prevent data providers from illegally providing the insured's private data, which is not allowed by law, to insurance companies.
- *Storage for random number generator.* Since the security feature of TEE ensures the validity of random number generation, we use the random number generator stored in TEE to generate random numbers that are needed in the cross-chain algorithm.
- *Key Escrow.* The TEE-based privacy-protecting key escrow relies on hardware isolation to provide underlying security protection for the blockchain system.

Blockchain layer We utilize blockchain to record data transfer process to satisfy our security needs of immutability and traceability. TEE is used as an execution environment rather than a storage environment since its storage space is limited. While blockchain, as a decentralized distributed ledger, naturally carries the 'trust gene' and is widely used for data storage and process management. Thus, we use blockchain to store the data and record the entire process to ensure immutability and traceability. As for cross-border insurance application scenarios, cross-border data transfer is often required. The traditional hash-locking algorithm is widely used in the field of asset exchange because of its atomicity, but it does not support the transfer of data. Therefore, we combine the hash-locking algorithm with the notary mechanism to enable secure data transfer in cross-border insurance business.

Application layer Our system involves three main users: the insured, data providers (e.g., hospitals) and insurance companies. In Figure 1, {*Data Provider*, *The Insured*, *Insurance Company*}_*inside* denotes data providers, the insured and insurance company inside the territory, and {*Data Provider*, *The Insured*, *Insurance Company*}_*outside* denotes data providers, the insured and insurance company outside the territory. We simplify the cross-chain process based on the characteristics of real-world users and we provide users with easy-to-use interfaces to create inquiry and invoke data cross-border transfer contracts.

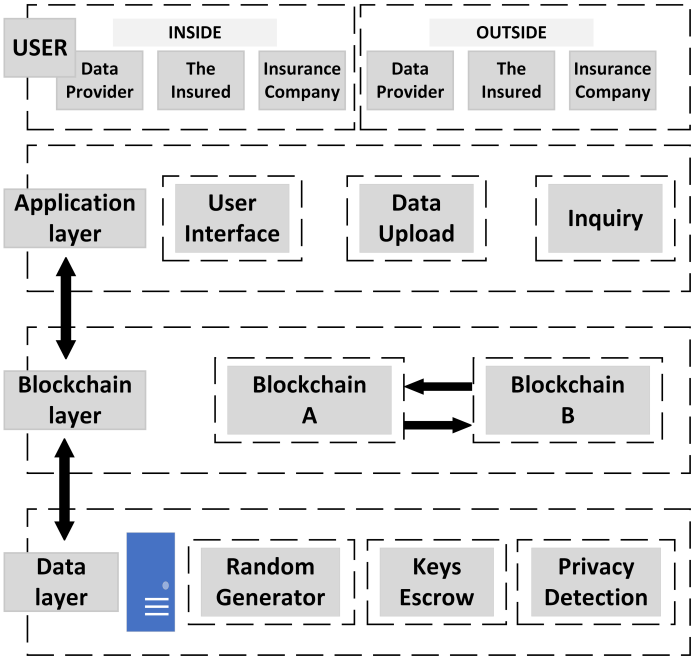

Figure 1. High-level architecture of the system.

5.3. System model

In this section, we offer a detailed explanation of the entire system operation process, with the system model depicted in Figure 2. In the cross-border insurance scenario, participants include data providers, the insured, and insurance companies both inside and outside the territory.

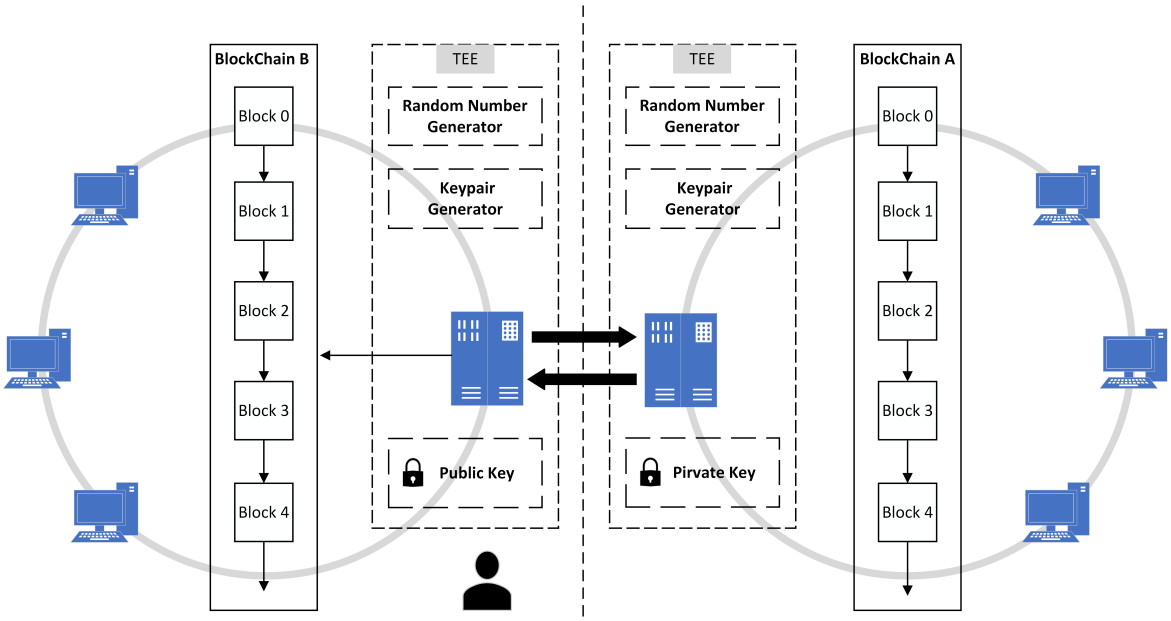

Figure 2. System model.

We assume that the insurance companies inside the territory jointly maintain a blockchain A, while the data providers outside the territory jointly maintain a blockchain B. For either blockchain A or blockchain B, each data provider or insurance company counts as a node in the blockchain. Each blockchain has a special node for handling cross-chain operations. This node has access to the blockchain but is not tasked with uploading data; its role is solely to

handle cross-chain requests and support the deployment of TEE functions. We implement some functions in the TEE, including privacy detection before uploading, random number generation, and key escrow.

The aim of our system model is to facilitate the exchange of data ownership on the blockchain across different regions. Specifically, we utilize the Hashed Time-Locked Contract (HTLC) to guarantee atomicity during cross-chain data transfer. Additionally, the TEE serves as the 'trusted third party', primarily ensuring that only authorized parties with ownership can decrypt the encrypted data.

6. Our proposed protocol

6.1. Data detection before uploading

To prevent the data provider from illegally uploading unauthorized sensitive data to the insurance company, we invoke a program deployed in TEE to perform the privacy detection before cross-chain data transfer. For instance, sensitive information such as the home address and ID number can be easily identified if included, and these information is not needed in the insurance claim. The data provider send the data to the TEE node for privacy detection before transferring it to the insurance company. We denote the data that needs to be detected before cross-border transfer process as $\mathbf{Data}_A$, and the data that will be uploaded to the blockchain system as $\mathbf{Data}_B$.

We apply checkPrivacy function to perform the sensitive information detection. Sensitive information within text can be detected through keywords matching and string formatting. For instance, regular expressions can be employed to detect whether mobile phone numbers, home addresses, ID numbers and other sensitive information are contained. This technology has matured in industry. AliCloud has already provide corresponding technical products. For sensitive information within images, Tran Lam et al. [78] proposed the PCNH model in 2016, utilizing convolution and object features to detect whether a photo contains private information.

Algorithm 1: Pseudo-Code of Privacy Data Detection

```
Initialize Provider, TEE Enclave, Blockchain
Function checkPirvacy( )
Function hashDigest( )
Data_A ← Provider send to Enclave
Data_B ← Provider upload to Blockchain
VERIFY Data_A.signature
IF Enclave.checkPirvacy(Data_A) == FALSE then
    return Pirvacy-Warning
ELSE
    RECORD hashDigest(Data_A)
ENDIF
VERIFY Data_B.signature
IF hashDigest(Data_B) == hashDigest(Data_A) then
    CALL Next-Step
ELSE
    return Difference-Warning
ENDIF
```

After the privacy detection, if the data does not include unauthorized sensitive data and is detected as compliant, it would be encrypted and return to the data provider after recording a hash digest of the data, otherwise the data would be returned to the data provider and is not allowed to be uploaded to the blockchain. The recorded hash digest of $\mathbf{Data}_A$ will be compared with the hash digest of $\mathbf{Data}_B$ to ensure the consistency of the detected data and the

data which is uploaded actually, that is, undetected data cannot be successfully uploaded. Only when the hash digest of the $\mathbf{Data}_A$ and the $\mathbf{Data}_B$ are identical, the data would be uploaded. Then the data provider will be authorized to proceed to the next step, the cross-chain data transfer process. The pseudo-code for privacy data detection process is shown in Algorithm 1.

6.2. Cross-chain technology

In this paper, we propose a protocol that integrates notary and hash-locking mechanisms for cross-border data transfer. First, we provide a brief introduction to the two mechanisms.

Notary mechanism enables a set of trusted nodes to act as the 'notary' to verify to the nodes of chain X that a particular event on chain Y has occurred. The notary mechanism is quite easy to implement among the mainstream cross-chain technologies. However, the realization of notary mechanism relies on a 'trusted third-party', which poses the risk of centralization; in other words, a group of elected notaries still have the potential to do evil [12]. Thus, security is a challenge for the notary mechanism.

Hash-locking mechanism utilizes hash-locks and time-locks to achieve atomic exchange. Hash-locking has a high level of security and transparency, making it easy to track and verify the status of transactions [16]. The security of the hash-locking mechanism depends on the security of the hash algorithm, so keeping the key in a secure manner becomes a top priority.

Considering security and ease of operation, we choose to combine the notary and hash-locking mechanism to propose an innovative cross-chain algorithm, which strikes the balance between operability and security, that is, it is as easy as possible to implement while ensure the security. This cross-chain algorithm and specific data transfer process will be discussed in Section 6.3.

6.3. Cross-chain data transfer

In this paper, cross-chain data transfer is to exchange the data ownership on different blockchains. The hash-locking algorithm was initially designed for the exchange of digital assets. We conceptualize data as an asset and utilize the hash-locking protocol combined with TEE to achieve secure cross-chain data transfer. The difference between 'cross-chain data transfer' and 'cross-chain asset transfer' lies in the requirement for data encryption before transfer and utilizing TEE as a security base to assist hash-locking mechanisms in ensuring security, whereas assets can be transferred directly without encryption.

The HTLC protocol is used to ensure atomicity. Without atomicity, the data provider, such as the hospital in health insurance, may refuse to provide the insured person's data upon receiving the receipt. In this case, the insurance companies have given the receipts but do not receive the corresponding data to settle claims. Conversely, if the hospitals provide the insured person's data but do not receive the receipts, then the insurance company could refuse to settle the claims.

In the traditional hash-locking algorithm, if Alice, a participant in blockchain A, intends to exchange assets with Bob, a participant in blockchain B, she needs to perform the following steps:

Step 1: Alice generates a random number S.

Step 2: Alice sends a hash of the random number S, denoted as $hash(S)$, to Bob, and agrees with Bob that the asset exchange will be performed hash-locked with $hash(S)$. The original random number S is required to unlock hash-lock.

Step 3: Alice initiates an asset transfer operation, transferring the asset on blockchain A to Bob with a hash-lock. The transferred asset is also time-locked; hence, if it remains unlocked beyond the agreed time, it will revert to Alice.

Step 4: After observing the asset transfer operation executed by Alice on blockchain A, Bob transfers the corresponding asset to Alice on blockchain B, similarly hash-locked

and time-locked.

Step 5: Alice uses the random number S to unlock the asset transferred by Bob on blockchain B.

Step 6: Bob gets the random number S on blockchain B and uses it to unlock the asset on blockchain A.

The above hash-locking algorithm follows the atomic exchange protocol. In other words, participants following the transaction process will make the transaction go smoothly, otherwise it will only harm their own asset rights. To address the security requirements of cross-border insurance scenarios, we integrate the notary mechanism and TEE security base to implement the following enhancements:

• **Signature verification.** To ensure the trustworthiness and traceability of data, it is necessary to verify the signature of the uploaded data on the blockchain. Signature verification is automated through the program deployed in the 'notary', the TEE node within the system. Failure to verify the signature prevents data from being uploaded to the blockchain. Algorithm 1 illustrates the function for signature verification.

• **Random number generation.** A simple and fixed random seed in the random number generation can enable attackers to predict and obtain the generated random numbers, which makes the generated random numbers used for hash-locking no longer secure. To ensure the validity and security of the generated random numbers, both cross-chain parties and the TEE node collectively contribute random number seeds, with the TEE serving as the trusted third-party 'notary' responsible for the random numbers generation. To be specific, the random number generator is deployed in TEE, utilizing the random seed for number generation. Algorithm 2 depicts the pseudo-code for random number generation.

• **Assistant to HTLC.** To enhance efficiency and prevent delays caused by non-compliance, the settings involved in hash-locking, such as the setup of time-locks, are generated by the 'notary', TEE node within the system. Algorithm 3 illustrates the pseudo-code for assisting the hash-locking algorithm.

• **Key Escrow.** To ensure the security and confidentiality of the keys, both the private and public keys are stored in the TEE. The process of key reception is realized through the secure channel between TEE and blockchain system. The procedure for establishing the secure channel will be elaborated in Section 6.4.

Algorithm 2: Pseudo-Code of Random Number Generator

```
Initialize TEE Enclave
Function RandomOperation( )
Function RandomNumberGenerator( )
Seed_E ← Enclave's random seed
Seed_P ← Provider's random seed
Seed_R ← Recipient's random seed
Seed ← RandomOperation(Seed_E, Seed_P, Seed_R)
Number ← Enclave.RandomNumberGenerator(Seed)
```

Algorithm 3: Pseudo-Code of Assisting the Hash-locking Algorithm

```
Initialize System Crosschain
Function setTimelock( )
Time_A ← Provider's average time-latency
Time_B ← Recipient's average time-latency
Transfer.timelock ← 2 * Time_A + 2 * Time_B
Receipt.timelock ← Time_A + Time_B
IF timeleft < 20% * timelock then
    SEND reminder message
ENDIF
```

The proposed cross-chain algorithm, which combines the hash-locking and notary mechanism, achieves a balance between security and ease of use. Given the need for efficiency and security while ensuring atomicity exchange, this cross-chain algorithm is particularly suitable for cross-border insurance data transfer tasks.The pseudo-code of the proposed cross-chain algorithm is shown in Algorithm 4. In general, the cross-chain algorithm consists of four phases:

(1) *Preparation phase.* The cross-chain process is triggered by data provider's request. Then TEE generates random *secret* which will be used later. (line 2-5 in Algorithm 4)

(2) *Hash-lock phase.* The provider and recipient both use $hash(secret)$ to set hash-locks. (line 6-10 in Algorithm 4)

(3) *Upload phase.* The provider and recipient upload the hash-locked encrypted data ($transfer$ in Algorithm 4) and the receipt of the encrypted data (*receipt* in Algorithm 4) with a time-lock to facilitate the exchange of the ownership of the hash-locked encrypted data and the receipt of the encrypted data using HTLC. (line 11-21 in Algorithm 4)

(4) *Unlock phase.* The recipient uses *secret* to unlock the hash-locked $transfer$ after the provider uses *secret* to unlock *receipt*. The provider gets the ownership of the receipt of the encrypted data and the recipient gets the ownership of the encrypted data. (line 22-30 in Algorithm 4)

Algorithm 4: Pseudo-Code of Cross-chain Process

Require: Provider.request, Recipient.request
Ensure: $transfer$.state, $receipt$.state
1: Initialize **Blockchain**$_A$, **Blockchain**$_B$, TEE **Enclave**, Cross-chain **System**
`/* generate random secret */`
2: **IF** Provider.*request*.TYPE == Claim **then**
3: VERIFY *request*.sender == Provider.address
4: *secret* ← **Enclave**.Random Function()
5: **ENDIF**
`/* hash-lock */`
6: hash(*secret*) ← **System**.Hash Function(*secret*)
7: *sender* ← Provider.address
8: *recipient* ← Recipient.address
9: Provider.data ← HashLock(Provider.data, hash(*secret*))
10: Recipient.data ← HashLock(Recipient.data, hash(*secret*))
`/* time-lock and upload */`
11: **IF** VERIFY Provider.input.signature == TRUE **then**
12: $t1, t2$ ← **System**.Set Timelock()
13: Provider.timelock ← $t1$
14: $transfer$ ← *sender*, *recipient*, Provider.data, $t1$
15: **Blockchain**$_B$.newblock ← $transfer$
16: **IF** VERIFY Recipient.input.signature == TRUE **then**
17: Recipient.timelock ← $t2$
18: *receipt* ← *recipient*, *sender*, Recipient.data, $t2$
19: **Blockchain**$_A$.newblock ← *receipt*
20: **ENDIF**
21: **ENDIF**
`/* unlock */`
22: **IF** Provider.*request*.TYPE == Unlock **then**
23: Provider ← UNLOCK (Recipient.data, *secret*)
24: Recipient ← S
25: **IF** Recipient.*request*.TYPE == Unlock **then**
26: Recipient ←UNLOCK(Provider.data,*secret*)
27: **return** *receipt*.state ← DONE
28: **ENDIF**
29: **return** $transfer$.state ← DONE
30: **ENDIF**

6.4. Security base: TEE

The notary mechanism is easy to implement. In terms of technical principles, the notary mechanism eliminates the need for expensive proof of work and complex proofs about the mechanism of interest, and it can flexibly support a variety of blockchains with different structures. Moreover, its more centralized processing model leads to higher processing efficiency. However, the principle of its algorithm requires a trusted third party to act as the 'notary', which makes the notary mechanism have the risk of centralization. In other words, a group of elected notaries still has the potential to do evil.

TEE can be a good solution to the centralization problem of notary mechanism. Based on a hardware-level isolation and secure boot mechanism, TEE builds a secure area (We call this secure area enclave in the rest of the paper). in the central processor where sensitive data and code are stored and can be computed. It is worth mentioning that the world outside the secure area cannot access the data in this isolated memory except through authorized interfaces. From technical point of view, TEE is naturally a 'trusted third party'. The separation kernel is the basic components of TEE [47], so it can provide the following isolation security assurance:

- *Data separation.* Data stored in the enclave cannot be read or tampered with by other partitions of the hardware.
- *Temporal separation.* The data in the public resource area will not disclose information about the data in any enclave.
- *Control of information flow.* There is no communication between the enclaves.
- *Fault isolation.* A security vulnerability in one enclave cannot propagate to other enclaves.

In addition, TEE is particularly noteworthy for its protection against system administrator privilege attacks, that is, even if the attacker gets root access, there is no way to get to the data and code in the enclave. Therefore, TEE is a natural and credible third party to act as the 'notary'. Thus, we combine the notary mechanism with TEE by storing the random number generator and keys in the TEE. Additionally, we let TEE act as the 'notary' to carry out the relevant verification to make up for the over-centralized defects of the notaries in the traditional notary mechanism. In this way we ensure the processing and computation efficiency while also providing security guarantee.

The process of data transfer and secure communication between the cross-chain system and TEE Secure Base in cloud servers is carried out through a secure channel, and the steps to build the secure channel are as follow:

Step 1: The cross-chain system in the cloud server claims a request to build a secure channel to the TEE node through the secure channel initialization interface.

Step 2: The secure channel construction request triggers the cross-chain system to claim a remote attestation request to the TEE node, then the cross-chain system obtains the remote attestation report carrying the public key information and verifies the remote attestation report to prove that the integrity of the TEE node has not been compromised.(In detail, TEE randomly generates a pair of public and private keys, and it sends the public key information to the cross-chain system's secure channel agent along with the additional information for the remote attestation report while caches the private key in memory.)

Step 3: The secure channel agent in the cross-chain system completes the key negotiation with the secure channel service at the TEE node based on the public key, and both parties obtain the session key to perform the encryption and decryption operations.

Step 4: After completing the secure channel construction, the cross-chain system can perform secure communication with the enclave in the server with TEE through the secure channel.

6.5. An example

We take the cross-border health insurance underwriting workflow as an example to illustrate the specific design of the system. To facilitate comprehension, let's consider a specific scenario: Alice, a resident of country A, frequently travels between country A and country B. She purchased a cross-border health insurance in country A. One day, she was admitted to a hospital in country B. After her recovery, she needed to initiate an insurance claim. The specific steps in the underwriting workflow are outlined in Figure 3.

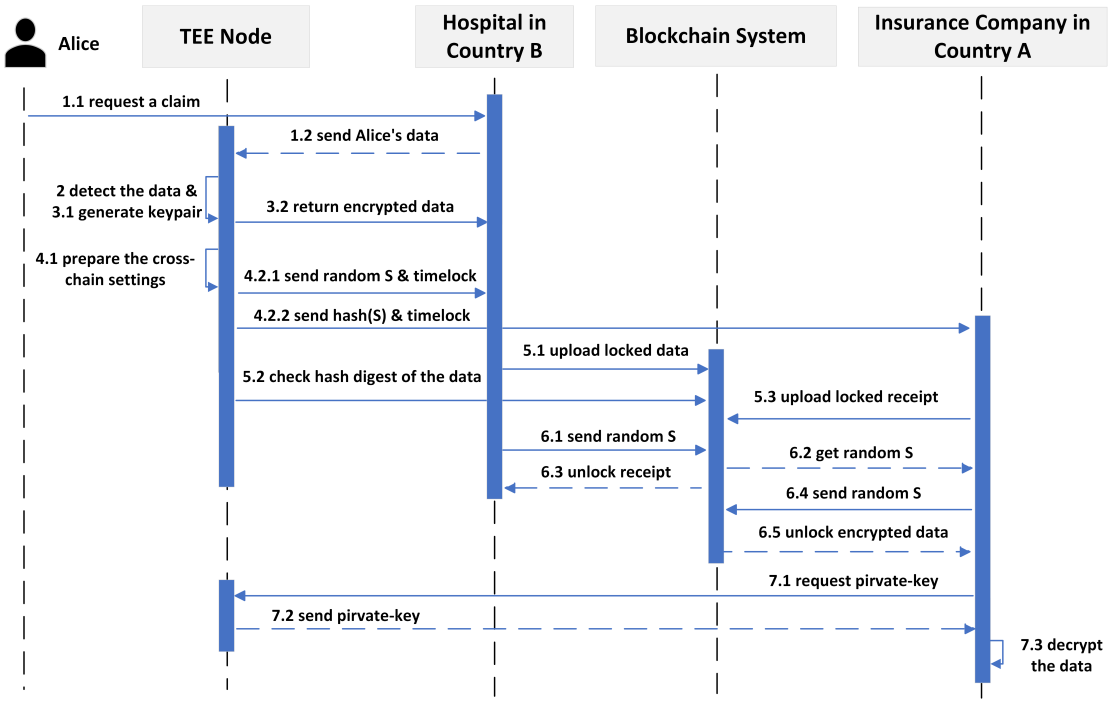

Figure 3. Cross-border health insurance underwriting workflow.

Step 1: *Claim and initialization.* Alice applies for a claim and authorizes the hospital in country B to provide her personal data, including physical condition and medical data, to the insurance company in country A. The hospital uploads Alice's data to the TEE node for privacy detection.

Step 2: *Check privacy compliance.* Alice's personal data is sent to the TEE node. After receiving data uploaded by the hospital, the TEE node checks whether it contains illegal information (see Section 6.1, Algorithm 1). If the hospital's uploaded data contains Alice's private information, it will be rejected by the TEE and the process aborts.

Step 3: *Key generation.* The TEE node generates a pair of keys for Alice: the public key is used for data encryption, and the private key stored within the TEE will be used for decryption later (see Section 6.3, Algorithm 2). The TEE node encrypts Alice's data with her public key and records the hash digest of the encrypted data. The encrypted data is then returned to the hospital.

Step 4: *HTLC preparation.* The TEE node initiates the cross-chain process by generating a random number S and setting a time-lock, as described in Section 6.3, Algorithm 3. The random number S and the time-lock are then sent to the hospital. The hash of S and the time-lock are then sent to the insurance company. Both the hospital and the insurance company then use the received parameters to set the hash-lock and time-lock in the blockchain system.

Step 5: *Lock and upload.* The hospital uploads Alice's personal data, encrypted by the public key, to chain B after setting a hash-lock and a time-lock. If the hash digest of the

encrypted data recorded in the TEE node matches the hash digest of the uploaded data in chain B, the signature verification is passed, and the encrypted data is successfully uploaded to the blockchain system. Otherwise, the TEE node will notify the insurance company to halt the subsequent process. The insurance company in country A then uploads the receipt with its signature to chain A which also contains the same hash-lock. At this step, the hospital can see the receipt on chain A, while the insurance company can see the encrypted data on chain B but cannot decrypt it.

Step 6: *Unlock.* The hospital uses the random number S to unlock the receipt on the blockchain system, so the insurance company gets the random number S which can be used to unlock the corresponding data before the expiration of the time-lock; otherwise, the data will be invalidated if the timeout period is exceeded.

Step 7: *Decrypt.* The insurance company sends a request to the TEE node to obtain Alice's private key to decrypt her personal data. The TEE node receives the request and checks whether the insurance company has ownership of the data by verifying it on the blockchain. If the insurance company owns Alice's data, the TEE node sends the private key to the insurance company for decrypting Alice's data.

Ensuring the trustworthiness of the data requires establishing a trusted access system for data providers. Only medical institutions that have successfully passed an audit are authorized to maintain the consortium chain of medical data. These institutions must sign, using their private keys, to endorse the uploaded data when uploading users' medical data, thereby enhancing the non-repudiation of the data. Medical institutions and insurance companies have established long-term cooperation and mutual trust to maintain this cross-border blockchain system. To safeguard against the leakage of users' private data, the data should be encrypted using users' public keys before uploading, and their private keys, stored within the TEE should be used for decryption after cross-chain data transfer.

7. Implementation and evaluation

7.1. Implementation

In the implementation section, our main objective is to verify the feasibility of our cross-chain transfer mechanism. The implementation of our cross-chain data transfer system operates independently of the underlying blockchain consensus algorithm. Considering that developing a blockchain system using *Java* offers advantages such as rapid development and customizability, we choose to implement the system prototype in *Java* to carry out the feasibility verification and provide a detailed examination of the entire system in this paper.

The experimental hardware environment comprises an Intel 12th-generation Core i7 processor paired with 16GB of RAM. Spring Boot version 3.2.1 is employed to deploy the blockchain system on port 8080 of the device. Furthermore, for RSA asymmetric encryption and the Elliptic Curve Digital Signature Algorithm (ECDSA), we utilize version 1.70 of the Bouncy Castle library.

The blockchain is an ordered list of objects of the Block class. The data format of one block on blockchain is shown below.

```
{
    "index":1456,
    "timestamp":1703937903747,
    "nonce":2015259534,
    "difficulty":4,
    "hash": "...",
    "previous_hash": "...",
    "transaction_hash": "...",
    "transactions": []
}
```

To enhance user convenience, we offer a graphical interface for system users. The available functions include initiating/decrypting data transfers/data receipts, mining a new block, and uploading data in JSON format. The user interface is illustrated in Figure 4.

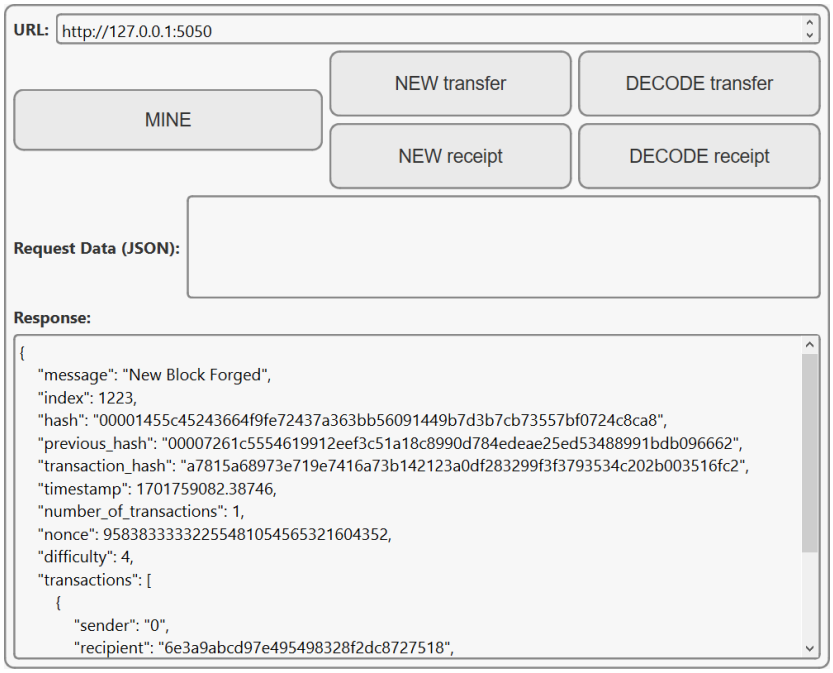

Figure 4. The user interface of the system.

To validate the TEE's function, we utilize an AliCloud server (model: g7t.large) equipped with an Intel Xeon 6398B processor. The server operates on Alibaba Cloud Linux 3.2104 LTS 64-bit version. Essential tools, such as the Software Guard Extensions Software Development Kit (SGX-SDK), have been installed on the cloud server. We utilize provided functions such as sgx_read_rand(), sgx_seal_data(), and sgx_unseal_data() to implement functionalities such as generating random numbers and sealing keys. The capabilities of the sgx_seal_data() and sgx_unseal_data() functions in sealing and unsealing data have been successfully verified, yielding the expected results.

```
[root@iZwz97jlmflmrpaskd66wdz test]# ./app
0x7ffce8186600
Seal succeed.
0x7ffce8186600
Unseal succeed.
[root@iZwz97jlmflmrpaskd66wdz test]#
```

7.2. Performance test

The time taken for a transaction to be recorded on the blockchain is significantly influenced by the Block Time of the blockchain. To minimize transaction waiting times, each transaction is promptly recorded on the blockchain upon receiving the request. Latency statistics for uploaded transaction data yielded the following results: The time from sending a transaction to its recording on the blockchain was measured 100 times. Most latencies were less than 0.6 seconds, with an average of approximately 0.45 seconds. The frequency distribution histogram of upload latency is illustrated in Figure 5.

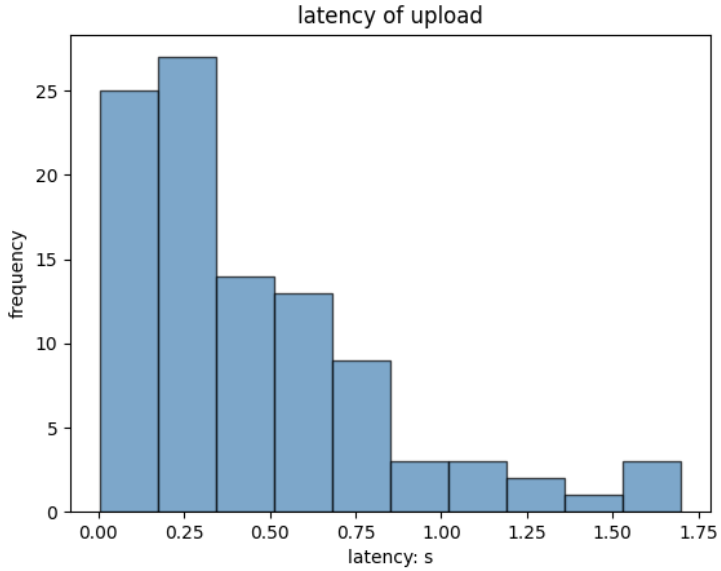

Figure 5. Latency of upload.

We assessed the feasibility of the blockchain cross-chain system by evaluating the latency in scenarios where transactions were initiated, receipts were promptly generated, and data unlocking was completed by both parties. After conducting 100 experiments, the average latency from transaction initiation to data unlocking was approximately 1.9 seconds. The frequency distribution histogram of transfer latency is illustrated in Figure 6.

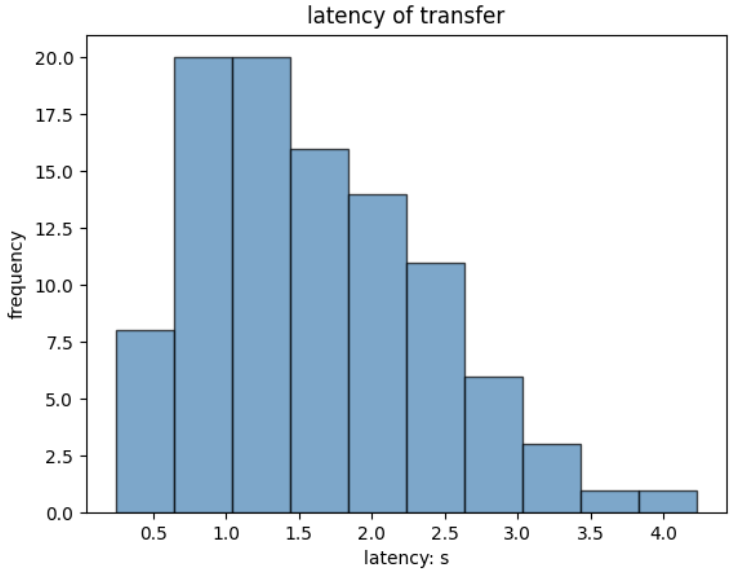

Figure 6. Latency of transfer.

The relationship between the latency of uploading and completing a cross-chain data transfer is apparent. Uploading requires the mining of one block, whereas a cross-chain data transfer involves four blocks, rendering the latter approximately four times longer than the former.

7.3. Security analysis

This section will discuss the attacks our solution can resist and the risks it may encounter.

The risk of centralization of notary mechanism. While the notary mechanism is easy to operate, its reliance on a centralized third party for verification introduces the risk of centralization. In essence, there is a risk of collusion among multiple notaries in the notary mechanism, where a group of elected notaries could engage in malicious behavior. Therefore, we propose integrating the notary mechanism with TEE technology. Specifically, we utilize TEE as the trusted third party and delegate key storage, random number generation, and privacy detection tasks to TEE. This approach effectively addresses the centralized risk problem of the notary mechanism by utilizing TEE's security properties.

Weak denial-of-service attack. A weak denial-of-service attack involves terminating data exchange between a data provider and a data recipient. In response to such attack, the system can record the number of times a participant terminates the exchange. If the number of terminations exceeds a certain threshold or frequency, the system can provide feedback to all participants in the blockchain, enabling them to jointly decide whether to continue cooperation.

Atomicity. Our solution for data transfer in cross-border insurance is based on a cross-chain algorithm, primarily combining the notary mechanism and hash-locking. The technical principles of time-locks and hash-locks in this improved cross-chain algorithm ensure atomicity of data transfer across the chain. Thus, our solution is an atomic swap protocol. Specifically, the data transfer process in the cross-border insurance business scenario has only two states: occurrence and non-occurrence, with no other intermediate states.

8. Conclusion

This paper presents a solution for data transfer in the cross-border insurance business scenario. First, we discuss the legal issues concerning data transfer in the cross-border insurance business and point out the inadequacy of existing laws. To address the challenges posed by legal restrictions and ensure legal compliance, we utilize cross-chain technology to facilitate cross-border data transfer. Considering the security of the hash-locking algorithm and the user-friendliness of the notary mechanism, we integrate these two cross-chain technologies to propose a cross-chain mechanism. The proposed cross-chain mechanism ensures both efficiency and security in data transfer across chains by guaranteeing atomicity in exchanges.

Building upon this proposed cross-chain mechanism, we present a system for implementing cross-border insurance. Within this system, TEE serves as a secure base and offers three main functions: random number generation, key escrow, and privacy data detection. TEE provides a secure enclave for storing and processing sensitive data through hardware-level isolation mechanisms. Furthermore, TEE protects against system administrator attacks, preventing unauthorized access to sensitive data stored within the TEE even if an attacker gains root privileges. The secure nature of TEE makes it an ideal candidate for a 'trusted third party'. By employing TEE as the 'notary', we mitigate the risk of centralization inherent in traditional notary mechanisms, thereby enhancing the security of cross-border insurance data transfer. We illustrate the system's user interface and validate the feasibility and security of the algorithm through extensive testing and analysis.

In our future work, we will delve deeper into the legal compliance of cross-border data transfer and endeavor to achieve a balance between security, efficiency, and ease of operation. Additionally, we will assess the performance of our system based on the improved cross-chain mechanism and TEE secure base in a real-world cross-border insurance application scenario.

Acknowledgments

We deeply appreciate the funding from Macau SAR Government FDCT Grant (0091/2020/A2), Shenzhen Science and Technology Plan Project (Shenzhen-Hong Kong-Macau Category C, No. SGDX20220530111001003) and Guangzhou-HKUST(GZ) Joint Funding Program (No. 2024A03J0630) to make this research possible.

Conflicts of interests

The authors declared that they have no conflicts of interests.

Authors' contribution

Conceptualization & Investigation, J.R., D.L.; Writing-original draft, J.R., D.L., Q.Z.; Writing-review & editing, J.R., D.L., Y.X., Q.Z., J.Y.; Project administration, Y.X., J.Y.; Supervision, Y.X., J.Y.; All authors have read and agreed to the published version of the manuscript.

References

[1] Focarelli D, Pozzolo AF. Cross-border M&As in the financial sector: Is banking different from insurance? *J. Bank. Financ.* 2008, 32(1):15–29.

[2] Van der Zwet A. In *The blurring of distinctions between financial sectors: fact or fiction?* Citeseer, 2003.

[3] Schoenmaker D, Sass J. Cross-border insurance in Europe: Challenges for supervision. *Geneva Pap. Risk Insur. Issues Pract.* 2016, 41:351–377.

[4] Zhang W. Development Trends of Financial Market Connectivity in Guangdong, Hong Kong and Macao Greater Bay Area. *China Exchange* 2023, 12(2023):68–70 (In Chinese).

[5] Jiang JX, Bai G. Evaluation of causes of protected health information breaches. *JAMA Intern. Med.* 2019, 179(2):265–267.

[6] Bode K. Facebook Leaked the Data of 533 Million Users and Didn't Tell Anyone. 2021. Available: https://www.vice.com/en/article/7k95qg/face-book-leaked-the-data-of-533-million-users-and-didnt-tell (accessed on 8 May 2024).

[7] Tasca P. Insurance under the blockchain paradigm. In *Business Transformation through Blockchain*, 1st ed. Cham: Palgrave Macmillan, 2019, pp. 273–285.

[8] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. Available: https://bitcoin.org/bitcoin.pdf (accessed on 8 May 2024).

[9] Wüst K, Gervais A. Do you need a blockchain? In *Conference Proceedings, 2018 crypto valley conference on blockchain technology (CVCBT)*, Zug, Switzerland, June 20–22, 2018, pp. 45–54.

[10] Raikwar M, Mazumdar S, Ruj S, Gupta SS, Chattopadhyay A, *et al.* A blockchain framework for insurance processes. In *Conference Proceedings, 2018 9th IFIP international conference on new technologies, mobility and security (NTMS)*, Paris, France, February 26–28, 2018, pp. 1–4.

[11] Kar AK, Navin L. Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telemat. Inform.* 2021, 58:101532.

[12] Ou W, Huang S, Zheng J, Zhang Q, Zeng G, *et al.* An overview on cross-chain: Mechanism, platforms, challenges and advances. *Comput. Netw.* 2022, 218:109378.

[13] Foundation F. Fusion Whitepaper: An Inclusive Cryptofinance Platform Based on Blockchain. 2017. Available: https://whitepaper.io/document/55/fusion-whitepaper (accessed on 8 May 2024).

[14] Xiong A, Liu G, Zhu Q, Jing A, Loke SW. A notary group-based cross-chain mechanism. *Digit. Commun. Netw.* 2022, 8(6):1059–1067.

[15] Thomas S, Schwartz E. A protocol for interledger payments. 2015. Available: https:

//interledger.org/interledger.pdf (accessed on 8 May 2024).
[16] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. 2016. Available: http://lightning.network/lightning-network-paper-DRAFT-0.5.pdf (accessed on 8 May 2024).
[17] Dilley J, Poelstra A, Wilkins J, Piekarska M, Gorlick B, *et al.* Strong federations: An interoperable blockchain solution to centralized third-party risks. *arXiv* 2016, arXiv:1612.05491.
[18] Guo Z, Liu L, Liang Z, Huang Y. Blockchain cross-chain technology research. In *Conference Proceedings, 2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Chongqing, China, December 16–18, 2022, pp. 1064–1070.
[19] Price WN, Cohen IG. Privacy in the age of medical big data. *Nat. Med.* 2019, 25(1):37–43.
[20] Brall C, Schröder-Bäck P, Maeckelberghe E. Ethical aspects of digital health from a justice point of view. *Eur. J. Public Health* 2019, 29(Supplement_3):18–22.
[21] Mitchell AD, Mishra N. Regulating cross-border data flows in a data-driven world: how WTO Law can contribute. *J. Int. Econ. Law* 2019, 22(3):389–416.
[22] Terry NP. Regulatory disruption and arbitrage in health-care data protection. *Yale J. Health Polcy, Law Ethics* 2017, 17:143.
[23] Arner DW, Barberis J, Buckey RP. FinTech, RegTech, and the reconceptualization of financial regulation. *Nw. J. Int'l L. & Bus.* 2016, 37:371.
[24] Packin NG. RegTech, compliance and technology judgment rule. *Chi.-Kent L. Rev.* 2018, 93:193.
[25] Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* 2018, 10(2):20.
[26] Shetty A, Shetty AD, Pai RY, Rao RR, Bhandary R, *et al.* Block chain application in insurance services: A systematic review of the evidence. *SAGE Open* 2022, 12(1):21582440221079877.
[27] Amponsah AA, Adebayo FA, WEYORI BA. Blockchain in insurance: Exploratory analysis of prospects and threats. *Int. J. Adv. Comput. Sci. Appl.* 2021, 12(1).
[28] Zhou L, Wang L, Sun Y. MIStore: a blockchain-based medical insurance storage system. *J. Med. Syst.* 2018, 42(8):149.
[29] Nizamuddin N, Abugabah A. Blockchain for automotive: An insight towards the IPFS blockchain-based auto insurance sector. *Int. J. Electr. Comput. Eng.* 2021, 11.
[30] Liu W, Yu Q, Li Z, Li Z, Su Y, *et al.* A blockchain-based system for anti-fraud of healthcare insurance. In *Conference Proceedings, 2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, Chengdu, China, December 6–9, 2019, pp. 1264–1268.
[31] Saldamli G, Reddy V, Bojja KS, Gururaja MK, Doddaveerappa Y, *et al.* Health care insurance fraud detection using blockchain. In *Conference Proceedings, 2020 seventh international conference on software defined systems (SDS)*, Paris, France, April 20–23, 2020, pp. 145–152.
[32] Zhang G, Zhang X, Bilal M, Dou W, Xu X, *et al.* Identifying fraud in medical insurance based on blockchain and deep learning. *Future Gener. Comput. Syst.* 2022, 130:140–154.
[33] Brophy R. Blockchain and insurance: a review for operations and regulation. *J. Financial Regul. Compliance* 2020, 28(2):215–234.
[34] Koens T, Poll E. Assessing interoperability solutions for distributed ledgers. *Pervasive Mob. Comput.* 2019, 59:101079.
[35] Yang D, Long C, Xu H, Peng S. A review on scalability of blockchain. In *Conference Proceedings, 2020 the 2nd International Conference on Blockchain Technology*, Hawaii,

USA, March 12–14, 2020, pp. 1–6.
[36] Qin K, Gervais A. An overview of blockchain scalability, interoperability and sustainability. *Hochschule Luzern Imperial College London Liquidity Network* 2018, pp. 1–15.
[37] Deng L, Chen H, Zeng J, Zhang LJ. Research on cross-chain technology based on sidechain and hash-locking. In *Lecture Notes in Computer Science*, Cham: Springer, 2018, pp. 144–151.
[38] Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, *et al.* Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J. Netw. Comput. Appl.* 2020, 149:102471.
[39] Hope-Bailie A, Thomas S. Interledger: Creating a standard for payments. In *Conference Proceedings, the 25th international conference companion on world wide web*, Montreal, Canada, April 11–15, 2016, pp. 281–282.
[40] Dehez-Clementi M, Lacan J, Deneuville JC, Asghar H, Kaafar D. A blockchain-enabled anonymous-yet-traceable distributed key generation. In *Conference Proceedings, 2021 IEEE International Conference on Blockchain (Blockchain)*, Melbourne, Australia, December 6–8, 2021, pp. 257–265.
[41] Zhao Z, Wu G, Susilo W, Guo F, Wang B, *et al.* Accountable identity-based encryption with distributed private key generators. *Inf. Sci.* 2019, 505:352–366.
[42] Anonymous. Wanchain - Building Super financial markets for the new digital economy. 2017. Available: https://www.wanchain.org/_files/ugd/9296c5_0d623032c67b4e2380e14452ec02a9e4.pdf (accessed on 8 May 2024).
[43] Dai B, Jiang S, Zhu M, Lu M, Li D, *et al.* Research and implementation of cross-chain transaction model based on improved hash-locking. In *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020*, Dali, China, August 6–7, 2020, pp. 218–230.
[44] Sun Y, Yi L, Duan L, Wang W. A decentralized cross-chain service protocol based on notary schemes and hash-locking. In *Conference Proceedings, 2022 IEEE International Conference on Services Computing (SCC)*, Barcelona, Spain, July 11–15, 2022, pp. 152–157.
[45] Han P, Yan Z, Ding W, Fei S, Wan Z. A survey on cross-chain technologies. *Distrib. Ledger Technol.* 2023, 2(2):1–30.
[46] GlobalPlatform. TEE system architecture. 2011. Available: https://globalplatform.org/specs-library/tee-client-api-specification/ (accessed on 8 May 2024).
[47] Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: What it is, and what it is not. In *Conference Proceedings, 2015 IEEE Trustcom/BigDataSE/Ispa*, Helsinki, Finland, August 20–22, 2015, pp. 57–64.
[48] Singh J, Cobbe J, Quoc DL, Tarkhani Z. Enclaves in the clouds: Legal considerations and broader implications. *Commun. ACM* 2021, 64(5):42–51.
[49] Li X, Zhao B, Yang G, Xiang T, Weng J, *et al.* A survey of secure computation using trusted execution environments. *arXiv* 2023, arXiv:2302.12150.
[50] Jauernig P, Sadeghi AR, Stapf E. Trusted execution environments: properties, applications, and challenges. *IEEE Secur Priv* 2020, 18(2):56–60.
[51] Bao Z, Wang Q, Shi W, Wang L, Lei H, *et al.* When blockchain meets SGX: An overview, challenges, and open issues. *IEEE Access* 2020, 8:170404–170420.
[52] Milutinovic M, He W, Wu H, Kanwal M. Proof of luck: An efficient blockchain consensus protocol. In *Conference Proceedings, the 1st Workshop on System Software for Trusted Execution*, Trento, Italy, December 12–16, 2016, pp. 1–6.
[53] Zhang F, Eyal I, Escriva R, Juels A, Van Renesse R. REM: Resource-Efficient Mining for Blockchains. In *Conference Proceedings, 26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, Canada, August 16–18, 2017, pp. 1427–1444.

[54] Li W, Andreina S, Bohli JM, Karame G. Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017*, Oslo, Norway, September 14–15, 2017, pp. 297–315.

[55] Saleh F. Blockchain without waste: Proof-of-stake. *Rev. Financ. Stud.* 2021, 34(3):1156–1190.

[56] Roy N, Shen S, Hassanieh H, Choudhury RR. Inaudible Voice Commands: The Long-Range Attack and Defense. In *Conference Proceedings, 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, Renton, WA, USA, April 9–11, 2018, pp. 547–560.

[57] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Conference Proceedings, 2016 IEEE symposium on security and privacy (SP)*, San Jose, California, USA, May 23–25, 2016, pp. 839–858.

[58] Yuan R, Xia YB, Chen HB, Zang BY, Xie J. Shadoweth: Private smart contract on public blockchain. *J. Comput. Sci. Technol.* 2018, 33:542–556.

[59] Cheng R, Zhang F, Kos J, He W, Hynes N, *et al.* Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *Conference Proceedings, 2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, Stockholm, Sweden, June 17–19, 2019, pp. 185–200.

[60] Bentov I, Ji Y, Zhang F, Breidenbach L, Daian P, *et al.* Tesseract: Real-time cryptocurrency exchange using trusted hardware. In *Conference Proceedings, 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, United Kingdom, November 11–15, 2019, pp. 1521–1538.

[61] Lan Y, Gao J, Li Y, Wang K, Zhu Y, *et al.* Trustcross: Enabling confidential interoperability across blockchains using trusted hardware. In *Conference Proceedings, 2021 4th International Conference on Blockchain Technology and Applications*, Xi'an, China, December 17–19, 2021, pp. 17–23.

[62] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016. Available: http://data.europa.eu/eli/reg/2016/679/oj (accessed on 8 May 2024).

[63] United States, Congress. Public Law 104-191, Health Insurance Portability and Accountability Act. 1996. Available: https://www.govinfo.gov/app/details/PLAW-104publ191 (accessed on 8 May 2024).

[64] Personal Information Protection Law (promulgated by the Standing Committee of the National People's Congress, Aug. 20, 2021, effective on Nov. 1, 2021) (P.R.C.). 2021.

[65] Cross-Border Privacy Rules (CBPR) System. 2011. Available: https://cbprs.org/documents/ (accessed on 8 May 2024).

[66] Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523(b) (2018). 2018. Available: https://www.law.cornell.edu/uscode/text/18/2523 (accessed on 8 May 2024).

[67] US Department of Justice. Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. 2019. Available: https://www.justice.gov/d9/pages/attachments/2019/04/10/doj_cloud_act_white_paper_2019_04_10.pdf (accessed on 8 May 2024).

[68] Hong Kong e-Legislation, Personal Data (Privacy) Ordinance. 2022. Available: https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf (accessed on 8 May 2024).

[69] Singapore, Personal Data Protection Act 2012. 2020. Available: https://sso.agc.gov.sg/Act/PDPA2012 (accessed on 08 May 2024).

[70] Cybersecurity Law (promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective on Jun. 1, 2017) (P.R.C.), 2017.
[71] Data Security Law (promulgated by the Standing Committee of the National People's Congress, Jun. 10, 2021, effective on Sep. 1, 2021) (P.R.C.), 2021.
[72] The Administration of Network Data Security (Exposure Draft) (promulgated by the Cyberspace Administration of China, Nov. 14, 2021, effective on Dec. 13, 2021) (P.R.C.), 2021.
[73] Measures for the Security Assessment of Outbound Data Transfer (promulgated by the Cyberspace Administration of China, Jul. 7, 2022, effective on Sep. 1, 2022) (P.R.C.), 2022.
[74] LMA Insurance Market Information Uses Notice. 2018. Available: https://lmg.london/wp-content/uploads/2023/12/LMA-Insurance-Market-Information-Uses-Notice-post-enactment-31-05-2018.pdf (accessed on 8 May 2024).
[75] Article 39 of Personal Information Protection Law (promulgated by the Standing Committee of the National People's Congress, Aug. 20, 2021, effective on Nov. 1, 2021) (P.R.C.), 2021.
[76] Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection. 2016. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed on 8 May 2024).
[77] Kim S, Han J, Ha J, Kim T, Han D. Sgx-tor: A secure and practical tor anonymity network with sgx enclaves. *IEEE ACM Trans. Netw.* 2018, 26(5):2174–2187.
[78] Tran L, Kong D, Jin H, Liu J. Privacy-cnh: A framework to detect photo privacy with convolutional neural network using hierarchical features. In *Proceedings of the AAAI conference on artificial intelligence*, Phoenix, Arizona, USA, February 12–17, 2016 .