Journal of Global Information Management
Volume 31 • Issue 7

A Consortium Blockchain-Enabled Evidence Sharing System for Public Interest Litigation

Wei Du, Renmin University of China, China
Hanxu Liu, Renmin University of China, China
Guannan Luo, China University of Political Science and Law, China*
Jiyuan Zhang, Renmin University of China, China
Wei Xu, Renmin University of China, China

ABSTRACT

Procuratorates, as the prosecutor in public interest litigation (PIL), need to obtain evidence from other PIL stakeholders including citizens, companies, governmental agencies, IoT monitoring devices and so on. However, the evidence sharing is not smooth due to the lack of secure data sharing and privacy protection during case investigation and evidence collection. Therefore, the authors propose a consortium blockchain-based secure data sharing and privacy protection scheme named PILChain. The involved organizations are connected as peers in PILChain. The safety of uploaded evidence and user privacy can be guaranteed with a fine-grained access control and zero-knowledge identity proof. InterPlanetary File System is introduced to store large evidence files off-chain, further enhancing the data security and system scalability. The security of PILChain is analyzed in terms of access control, evidence confidentiality, evidence integrity, traceability, privacy, and scalability. Last, the authors evaluate the performance of the developed prototype system by implementing PILChain on Hyperledger Fabric.

KEYWORDS

Consortium Blockchain, Data Sharing, Hyperledger Fabric, Privacy Protection, Public Interest Litigation

INTRODUCTION

Public interest litigation (PIL) refers to the litigations in which the relevant organizations sue the court for the violation of the law, which has caused de facto damage or potential damage to state or social public interest, which plays an important role in the civil justice system. Unlike private litigations, only procuratorates and other organizations prescribed by law are qualified to prosecute in PIL (Y. Wang & Xia, 2023). As a special form of litigation, the PIL has received increasing attention from the state and society (Holladay, 2012; Wenjun Yan, 2021). It has helped address a number of problems such as pollution (Jain, 2022), terrorism, government corruption, and women's and children's rights (Paraschiv, 2011; Samuels, 2018; Xie & Xu, 2022; Yap & Lau, 2011). In

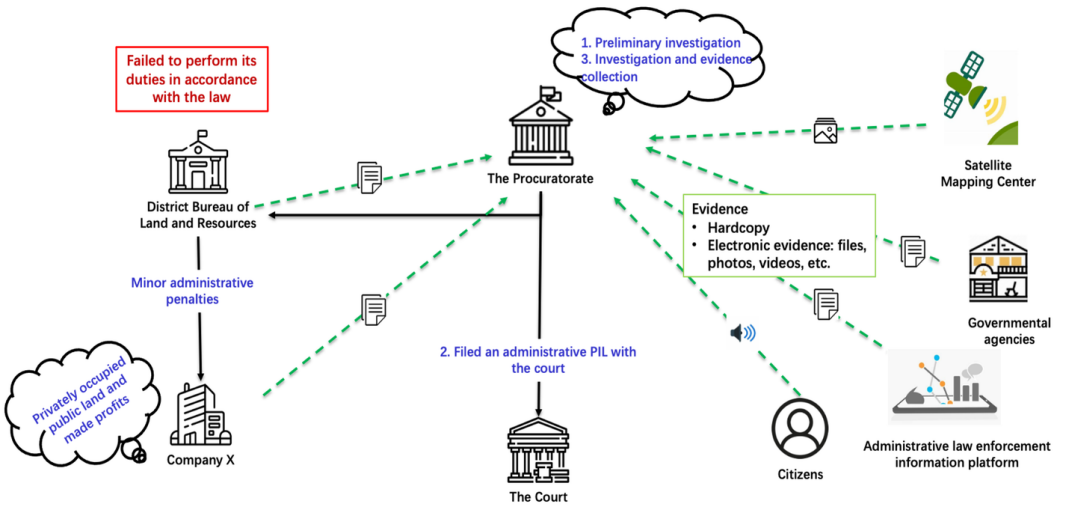
DOI: 10.4018/JGIM.330422 *Corresponding Author

China, procuratorates filed about 169,000 PIL cases in the year 2021 alone[1], and environmental public interest litigation in China has entered a booming period and made great progress (A. L. Wang & Gao, 2010; Zhuang & Wolf, 2021).

Figure 1 shows a real-world example of an administrative PIL filed by the procuratorate. Company X privately occupied public land and built a parking lot to make profits without the approval of the District Bureau of Land and Resources. Upon preliminary investigation, the procuratorate found that the district bureau failed to perform its duties in accordance with the law and therefore filed the administrative PIL with the court. The procuratorate then initiates case investigation and evidence collection. The PIL evidence can be collected from the district bureau, the company, other governmental agencies, IoT devices, citizens, and so on.

However, current PIL faces challenges due to the lack of secure data sharing and privacy protection during case investigation and evidence collection. On one hand, evidence collection in PIL investigations can be quite difficult (Yi Wang et al., 2022; Zhu et al., 2023). Given the lack of existing information interconnection between different organizations involved in a PIL case, the evidence providers are often reluctant to disclose related information considering the risk of information leakage or the fear of public monitoring. For example, Zhu et al (2023) found that local officials reduce information disclosure in PILs to avoid public monitoring (Zhu et al., 2023). Even between governmental agencies, data sharing is not smooth due to the data privacy and trust problem. Individual evidence providers are even fearful of revealing identity information and being retaliated against maliciously (Agrawal & Bhalotia, 2022), e.g., Wal-Mart fired employees who reported the use of "black oil" (Sirui & Zhihui, 2015), and qui tam actions come from former employees due to the fear of retaliation (Hurwitz, 2019). Even though the courts and procuratorates have the obligation to protect informants or witnesses from physical harm, the current system cannot fully protect the privacy and security of evidence providers, as their information may be disclosed by internal staff. On the other hand, the storage and preservation of evidence are not guaranteed. The gradually increasing electronic evidence files, such as Internet trail information, satellite remote sensing maps, and network media opinion, are often stored on individual computers or on the Internet (Hegarty et al., 2014; Oatley, 2022; Taylor et al., 2010). Such a centralized storage system easily causes risks of information leakage, tampering, or hacker attacks, thus authenticity and integrity are not guaranteed when electronic evidence is arbitrarily modified or damaged (Casey, 2002; Wenqi Yan et al., 2020). Developing blockchain technology can alleviate these challenges.

Figure 1. An Example of an administrative PIL filed by the procuratorate



The decentralized data storage in blockchain mitigates the issue of hacker attacks in conventional centralized databases, and the blockchain data structure is capable of protecting the evidence authenticity and integrity (Chen et al., 2020; Wu & Zheng, 2020). Therefore, blockchain has been introduced to maintain and trace electronic evidence in judicial practices given its advantages in guaranteeing transparency, authenticity, security, and auditability (Lone & Mir, 2019; Wenqi Yan et al., 2020). In 2018, UK courts started piloting the blockchain evidence system[2]. The blockchain system ensures evidence integrity by providing verifiable records and reduces the risk of evidence tampering by providing cryptographically verifiable forms of data. At present, in China, many cities such as Hangzhou, Beijing, and Guangzhou have established Internet courts and set up judicial blockchain systems to store electronic evidence. However, existing judicial blockchain systems mainly solved the problems of electronic evidence storage and preservation for general litigation practices (J. Guo et al., 2022; Li et al., 2021; Tian et al., 2019), while data sharing between judicial stakeholders and personal privacy protection, which matter in PIL, were not yet solved.

To ensure the secure data sharing and privacy concern in PIL, the authors hereby propose a decentralized secure consortium blockchain system for PIL practices, i.e., PILChain, using a permissioned blockchain platform—Hyperledger Fabric. By connecting involved organizations, such as third-party evidence platforms, governmental agencies, procuratorates, and courts as peers (nodes), in consortium blockchain, this system enables PIL stakeholders, including evidence providers and requesters, to upload and access evidence data privately and securely. Different types of PIL stakeholders have different permissions for data usage as established through certificate authority (CA) and access control. Further, an InterPlanetary File System (IPFS) is introduced to store large evidence files off-chain, which further enhances data security and system scalability. PILChain also introduced Identity Mixer, a cryptographic protocol suite for privacy-preserving authentication, to protect evidence providers' personal identity or other attributes with zero-knowledge proof. Last, the authors perform system analysis on the PILChain in terms of access control, evidence confidentiality, evidence integrity, non-tamperability, traceability, non-repudiation, privacy, and scalability. In addition, they developed a prototype system based on Hyperledger Fabric and used Apache JMeter to perform simulation and analysis. Experimental results showed the stable performance of the PILChain in dealing with the increasing number of requests for evidence upload and evidence acquisition.

The contributions of this paper are:

- The designing of a permissioned consortium blockchain system for PIL practice using Hyperledger Fabric.
- The fine-grained access control in the PILChain allows different PIL stakeholders to have different permissions on evidence data.
- The combination of IPFS and blockchain enables transmitting evidence efficiently over consortium blockchain.

The remainder of this paper is organized as follows. The literature review section provides related work. The next section provides the workflow and core components of the PILChain, followed by a section that uses a real-world PIL case to illustrate the implementation of the PILChain. System analysis and experimental evaluation of the prototype system are then provided, followed by conclusions and future work, which are provided in the last section.

LITERATURE REVIEW

The present study is about secure data sharing and privacy protection in public interest litigation. The authors first surveyed the prior studies relating to blockchain applications for secure data sharing and privacy protection. The application field was extended to healthcare, smart city, and judicial fields.

Blockchain for Secure Data Sharing and Privacy Protection

Blockchain can be understood as a distributed decentralized ledger for recording transactions in a peer-to-peer (P2P) network. A blockchain system has several built-in security features (e.g., cryptography, consensus, smart contract, and identity control) that help ensure data immutability, efficient decentralized transactions, data integrity, and user anonymity (Nofer et al., 2017). First, in blockchain, different transactions (e.g., cryptocurrency transactions) are "packed" into blocks that are interconnected in a linear, chronological way to form a virtual chain (Crosby et al., 2016). The modification of any block will change the hash value that will not validate with the hash value stored in the next block, which ensures immutability. Second, the use of consensus mechanisms allows the maintenance of a consistent ledger on blockchain by relying less on third parties. Applications such as data sharing and transactions can be decentralized and efficient. Third, blockchain uses asymmetric cryptography to protect the integrity of data (Härdle et al., 2020). Asymmetric cryptography uses keypairs, i.e., a public key and a private key, for data encryption and data decryption, ensuring the transmission of secure messages between two or more parties. Fourth, although blockchain transactions are made public to all users, blockchain users can remain anonymous without disclosing off-chain identity information or other transactions (Yli-Huumo et al., 2016).

The aforementioned security features of blockchain make it a popular technology for secure data sharing and privacy protection in a wide range of areas (Fan et al., 2018; Patel, 2019; A. Zhang & Lin, 2018). Due to the limited number of related studies in the judicial field, the authors also reviewed similar studies in other fields such as healthcare and smart city. For example, Patel (2019) developed a blockchain framework for cross-site medical image sharing to eliminate third-party intermediaries. By using the asymmetric cryptography of blockchain in identity verification and user authentication while preserving privacy, the proposed framework solves the problem of cross-site identity matching and anonymity required by an interoperable health system. Fan et al. (2018) proposed a blockchain system named MedBlock to allow efficient access and retrieval of sensitive medical records with an improved consensus mechanism to avoid network congestion caused by patients visiting hospitals in a concentrated time. Zhang and Lin (2018) designed a blockchain-based system that uses both private blockchain and consortium blockchain for personal health information (PHI) sharing to enable the cross-hospital search with secure indexes.

In recent years, technologies, including storage technology (Liang et al., 2017; Shen et al., 2019), access control (Makhdoom et al., 2020), and privacy-preserving computation (Y. Gao et al., 2020; S. Guo et al., 2020; Xu et al., 2022; W. Zhang et al., 2021; Zheng et al., 2018) were combined with blockchain to further improve the security of data access. For example, MedChain proposed by Shen B. et al. (2019) contains both a blockchain and a P2P storage network in order to keep the consistency and integrity of medical records after updating and maintenance. Liang X. et al. (2017) used blockchain to assist in access control of individual health data by recording access requests from healthcare providers and validating them through a permission management protocol. To alleviate the privacy threats in the Internet of Things (IoT) systems, Makhdoom I. et al. (2020) partitioned the blockchain network into different channels to handle specific types of data and managed the data access requests through access control to achieve secure data sharing. To deal with the problems of malicious nodes and differential attacks on city data, S. Guo et al. (2020) combined federated learning and blockchain over the smart city, where federated learning protects data privacy by sharing model parameters instead of original data while blockchain ensures data trust among multi-parties. Proxy re-encryption (PRE) technique, as a special type of public key encryption, further ensures the secure sharing of sensitive data (Manzoor et al., 2019). Y. Gao et al. (2020) proposed a blockchain-based data-sharing framework that combines identity-based PRE to secure device-to-device communication in smart cities (Y. Gao et al., 2020).

Moreover, blockchain technology enables decentralization, immutability, and traceability, and therefore provides an operating environment for programmable contracts (Lin et al., 2022). Smart contracts in blockchain support the automatic implementation of algorithms, custom logic, and

trustworthy transactions. They have been widely used in financial transactions (Debe et al., 2020), Internet of Things (Sultana et al., 2020), and supply chain management (Dolgui et al., 2020). Prior studies have also utilized smart contracts for data sharing and privacy protection. For example, it has been confirmed that smart contracts can effectively achieve distributed trust management and access control in data sharing (Javaid et al., 2019), or customization of data sharing policies with less cost (Rahman et al., 2020). It also supports patients to selectively share data with doctors in order to protect patient privacy and rights (Zaghloul et al., 2019). In the proposed solution, key sectors such as authentication of organizational members and access control of evidence data can be clearly defined with smart contracts.

Judicial Blockchain System

In the judicial field, prior studies related to blockchain focus on electronic evidence storage and electronic law records management. In recent years, great efforts have been made to enhance the secure evidence transmission between various departments or stakeholders in judicial procedures with the support of blockchain (J. Guo et al., 2022; Tsai, 2021). Different smart contracts for sending, calling, and querying evidence were designed in blockchain (J. Guo et al., 2022). Access control in evidence creation, transfer, and modification can further ensure evidence security (Tsai, 2021). Many blockchain solutions were proposed to store and trace electronic evidence in the process of forensic investigations. Considering the design of blockchain in ensuring integrity, transparency, authenticity, security, and auditability, Lone and Mir (2019) proposed a blockchain-based digital forensics chain of custody to maintain and trace digital evidence in the forensic community. Billard (2019) proposed a blockchain-based digital evidence inventory to store evidence in a digital forensic investigation (Billard, 2019). To ensure the integrity and traceability of digital evidence, Yan et al. (2020) proposed a blockchain-based digital evidence chain of custody (Yan et al., 2020). Specifically, they introduced attribute-based encryption to achieve fine-grained access control and BLS signature to verify digital evidence. López-Aguilar and Solanas (2021) proposed a blockchain solution to facilitate the cross-border exchange of digital evidence in the investigation process of fighting against cybercrimes (López-Aguilar & Solanas, 2021). However, prior studies mainly designed for general litigations can only partially satisfy the needs of evidence transmission in PIL investigations, while specific problems in PIL are not yet solved. For example, PIL involves several institutions, and permissions vary for different users from different institutions, while prior studies (Lone & Mir, 2019; Yan et al., 2020) assume the evidence handling by different parties is the same, which is inconsistent with the scenario of PIL. Fine-grained data access in PIL was not fully addressed. Therefore, a blockchain solution for evidence upload and query in PIL investigation is required.

In addition, user privacy protection is critically important in PIL, which is different from general litigations, making the applicability of the general judicial blockchain system limited in PIL scenarios. Few studies have investigated the privacy protection of relevant stakeholders in judicial procedures. For example, Li et al. (2021) introduced the use of short randomizable signatures as a zero-knowledge identity proof to anonymously verify the identity of evidence providers in order to protect witness privacy, and designed a secure voting method to protect the privacy of jurors in courtroom trials (Li et al., 2021). A voting method that involves a judge may be less convenient in evidence investigation. Therefore, the authors used a similar zero-knowledge identity proof to authenticate the digital identities without revealing private user information in PIL cases.

In addition to the demand for secure evidence transmission, there are many large-size electronic evidence files, such as high-resolution pictures, audio, and videos, in forensic investigations, which caused performance degradation of blockchain systems. Therefore, several studies have combined blockchain systems with off-chain storage systems such as IPFS to improve the access efficiency of large-scale electronic evidence or law records (Philip & Saravanaguru, 2022; Tian et al., 2019; Verma et al., 2021). Take the vehicle accident as an example, evidence data from nearby vehicles, witnesses, and cameras will be aggregated and uploaded to IPFS, and blockchain is used to store IPFS

file identifiers for safe access (Philip & Saravanaguru, 2022). Kim et al. (2021) proposed a two-level blockchain system where frequently changed information in criminal investigations is stored in the hot blockchain and large files such as videos are stored in the cold blockchain (Kim et al., 2021). The design ensures the performance of a blockchain system when storing large evidence files. Given that the evidence storage in IPFS overcomes the centralized storage problem and the efficient and secure data sharing via IPFS over blockchain, the authors introduced IPFS as the off-chain storage system by following prior studies (Athanere & Thakur, 2022; Philip & Saravanaguru, 2022).

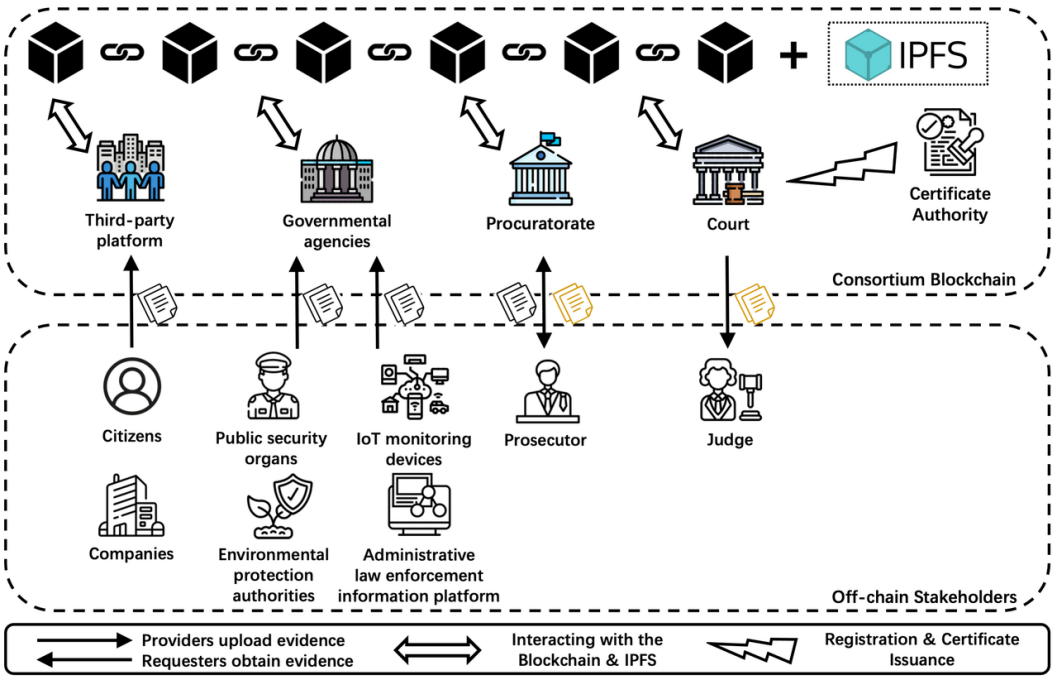
PILCHAIN: CONSORTIUM BLOCKCHAIN SYSTEM MODEL FOR PIL PRACTICE

Model Overview

Figure 2 shows the proposed consortium blockchain-system model for PIL practice based on Hyperledger Fabric, i.e., the PILChain. Hyperledger Fabric is an open-source permissioned blockchain framework that supports memberships based on permission (Kim et al., 2021; Liu et al., 2020). With Fabric, stakeholders in PIL can share electronic evidence in a separate environment and therefore ensure evidence security and integrity. The consortium blockchain consists of organizational members involved in PIL case investigation, including third-party evidence platforms, governmental agencies, procuratorate, and court. Off-chain PIL stakeholders, e.g., citizens, companies, public security organs, environmental protection authorities, IoT monitoring devices, prosecutors, and judges, can upload/access evidence via corresponding organizations. To ensure the efficiency of evidence management, the PILChain only reserves evidence metadata on-chain and uses IPFS, a peer-to-peer storage network for storing and sharing data securely in a distributed file system (Benet, 2014), to store large evidence files off-chain.

There are two key user roles in evidence investigation, i.e., evidence provider and evidence requester. As shown in Figure 2, the evidence provider uploads evidence, and the evidence requester

Figure 2. System model for PIL practice based on hyperledger fabric



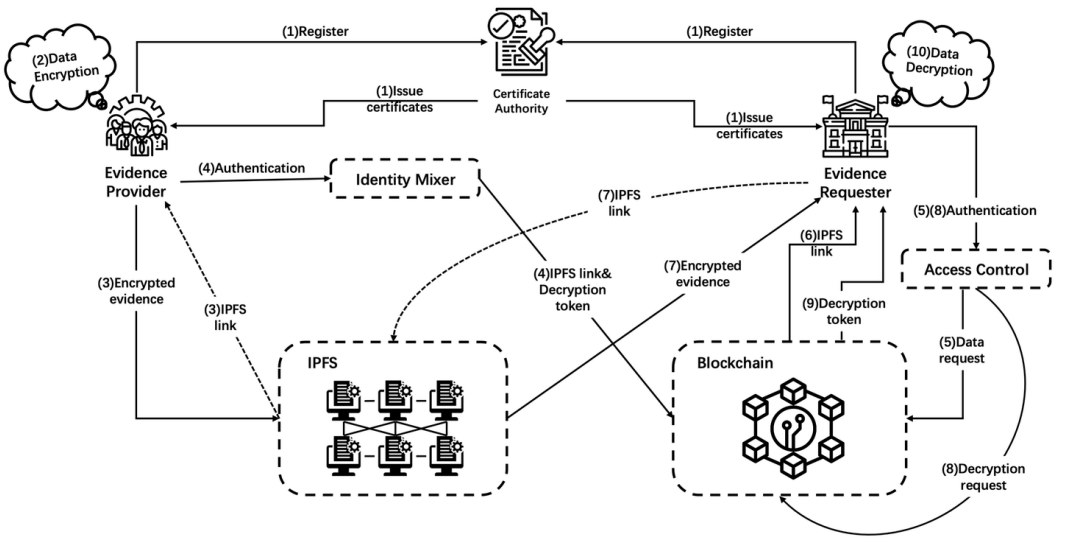
requests and obtains evidence on the consortium blockchain. The corresponding real-world stakeholders and permitted operations in the system are summarized as follows.

- **Evidence Provider:** Refers to any stakeholder who holds evidence related to a PIL case. They can be members from third-party evidence platforms, governmental agencies, and the procuratorate. Evidence from citizens and companies can be recorded through third-party evidence platforms or public security organs. Other governmental agencies related to a PIL case investigation, such as environmental protection authorities, can share their data with a procuratorate and court. The system also enables automatic data access from IoT devices, including satellite remote sensing and environmental monitoring devices. Historical law enforcement information can be accessed from administrative law enforcement platforms. Procuratorate investigators can also upload evidence during case investigations. For uploaded evidence, the PILChain first encrypts evidence data locally and stores the encrypted data in IPFS. Metadata of the PIL evidence, including link address and decryption token, are stored in the consortium blockchain.
- **Evidence Requester:** A court and a procuratorate are primary evidence requesters. Evidence requesters send evidence requests through blockchain, which is verified by Access Control to obtain the corresponding IPFS link address and decryption token. The encrypted evidence data can then be downloaded from IPFS. Using a decryption token, decrypted evidence data will be sent to the evidence requesters.

The overall workflow of the PILChain, including evidence upload and evidence acquisition, is summarized in Figure 3.

1. First, both evidence providers and evidence requesters need to register with CA, which issues digital certificates in Hyperledger Fabric. With issued digital certificates and private keys, they obtain the authority to perform certain operations in the consortium chain.
2. An evidence provider uploads evidence, and the PILChain encrypts the evidence data locally using a symmetric encryption algorithm.
3. The PILChain uploads the encrypted evidence to IPFS and receives a returned address link.

Figure 3. The overall workflow of the PILChain



4. The PILChain uploads the IPFS address link and the decryption token to the consortium blockchain in the form of a transaction. The evidence provider in this process can use Identity Mixer for privacy protection. As a cryptographic protocol suite in Fabric, Identity Mixer can verify the identity of evidence providers without exposing private information, ensuring the anonymity of the evidence submission.
5. An evidence requester sends a request to the consortium blockchain for evidence acquisition, during which Access Control verifies the attributes and grants permissions.
6. If the verification succeeds, the consortium blockchain returns the IPFS address link.
7. The PILChain uses the IPFS link to obtain the corresponding encrypted evidence from IPFS.
8. A request is then sent to the consortium blockchain to obtain the decryption token, during which Access Control verifies the attributes and grants permissions.
9. If the verification succeeds, the consortium blockchain returns the decryption token.
10. The PILChain obtains the decrypted evidence and returns it to evidence requesters.

The workflow can be roughly divided into three key components: user registration, evidence encryption, evidence upload, and evidence acquisition. In addition, the system ensures the privacy protection of evidence providers during evidence upload and implements access control to achieve fine-grained access during evidence acquisition. All these functions can be implemented through smart contracts. The details are provided as follows.

User Registration

In consortium blockchain, each organization has a corresponding CA administrator who is responsible for the joining of new members in the organization and the authentication of existing members. For user registration, first, the system checks if the user with the id "userID" has been enrolled. If not, the user can register as a new member by submitting personal identity information. Accordingly, CA generates a *secret* for the user by assigning *role* and attributes required by the user. Next, CA returns a digital *certificate* to the user and the corresponding public/private key pair, indicating that the user has successfully registered. The digital certificate owned by the user contains the information as to which organization the user belongs. The private key is kept separately by the user.

Evidence Encryption and Evidence Upload

The PILChain uses IPFS to store evidence data off-chain. As a distributed file system for storing and sharing data, IPFS splits evidence data into smaller chunks, enabling the storage of large evidence data. With IPFS, the PILChain only needs to store small metadata on-chain, which enables scalable data sharing.

An evidence provider uploads evidence *evi* of data type *eviType* for a PIL case *caseID* to the PILChain. Figure 4 describes the process of providing evidence on the blockchain. The system encrypts the evidence locally using the Advanced Encryption Standard (AES) algorithm before it is uploaded to IPFS, during which users can choose to set their own encryption password *secretToken* or let the system assign it randomly. AES is a symmetric encryption algorithm. Next, the encrypted evidence data is uploaded to IPFS, and IPFS generates its file link address *ipfsaddr*.

The PILChain automatically generates a unique identifier *eviID* for the new evidence uploaded to IPFS. First, the PILChain packs evidence information including *userID*, *eviID*, *eviType, and caseID* into a composite primary key *Keys*. Then, the IPFS link address *ipfsaddr* for encrypted evidence and encryption password *secretToken* are written to the blockchain using the function *WriteLedger()*, with the composite primary key *Keys* as their unique identifier. This design ensures the password *secretToken* matches the corresponding evidence.

Figure 4. Pseudo code of evidence encryption and evidence upload

```
Function 1: provideEvidence()
Input: args{caseID, userID, eviID, eviType}, ipfsaddr, secretToken
Output: bool
BEGIN
    evidenceData ← {ipfsaddr, secretToken}
    Keys ← args{caseID, userID, eviID, eviType}
    //Write the evidence to the blockchain, with 'Keys' as its unique identifier
    err = WriteLedger(stub, evidenceData, Keys)
    if err != NULL then
        return Error('Evidence upload error!')
    else
        return Log('Success in uploading evidence!')
    endif
END
```

Privacy Protection for Evidence Providers

For each organization that will upload evidence, the authors create Idemix Membership Service Providers (MSP) as Verifier. Users in an organization will get a digital certificate with the Idemix function after registration. Users can submit *proof* to Idemix MSP with zero-knowledge proof to verify identity or attributes. To further explain, Idemix MSP can verify that the user belongs to this organization without revealing other attributes, thus hiding private information when uploading evidence. Meanwhile, Idemix credentials themselves are unlinkable. With zero-knowledge proof, neither Fabric CA nor Idemix MSP can link the *proof* to a user's original credentials, nor can they distinguish whether two different *proofs* come from the same user. In other words, even if a user uploads multiple pieces of evidence, one cannot obtain user information that has not been disclosed by using certificate information. This design ensures privacy preservation and anonymity protection of evidence providers.

Evidence Acquisition

The PILChain enables users (e.g., procuratorate and court) with permission to retrieve evidence data through *caseID*. Figure 5 describes the process of evidence acquisition. The *ReadLedger()* function performs a fuzzy search on the blockchain with the query *caseID* typed by a user. A list of evidence on the PILChain is retrieved. Then, if an evidence requester wants to access the evidence, the PILChain first verifies the evidence requester's identity through access control contract. If the verification passes, the system uses the IPFS link address to obtain the encrypted evidence from IPFS. It further performs identity verification through the access control contract to obtain a decryption password *secretToken*. With *secretToken*, the original evidence data can be transmitted to the evidence requester.

Access Control

The PILChain adopts strict data access control. An evidence provider can only access evidence uploaded by himself, while evidence requesters with permissions can access all the evidence in the PILChain. Different user roles have different permissions in the PILChain system, which is provided in Table 1. As evidence providers, the third-party platforms and governmental agencies have permission to upload and query evidence, but can only decrypt and access the evidence they themselves have uploaded. In addition to the above permissions, evidence requesters, including the procuratorate and court, can access evidence uploaded by other organizations on the blockchain.

For a user who tries to access evidence data, access control first identifies whether the user comes from an organization with permissions. For organizations that have access to evidence data, the user's request is permitted directly. The PILChain gets the corresponding IPFS link *ipfsaddr*

Figure 5. Pseudo code of evidence acquisition

```
Function 2: queryEvidence()
Input: caseID
Output: bool
BEGIN
    partialKey ← caseID
    // According to the case under investigation to query
    {results, err} = ReadLedger(stub, 'caseID', partialKey)
    if err != NULL then
        return Error('No evidence of this case!')
    endif
    // Get a list of evidence
    for result in results do
        err = json.Unmarshal(result, &evidence)
        if err != NULL then
            return Error('Evidence query error!')
        endif
        evidenceList = append(evidenceList, evidence)
    endfor
    return Log('Success in querying evidence!')
END
```

Table 1. Operation permissions of related stakeholders in the PILChain

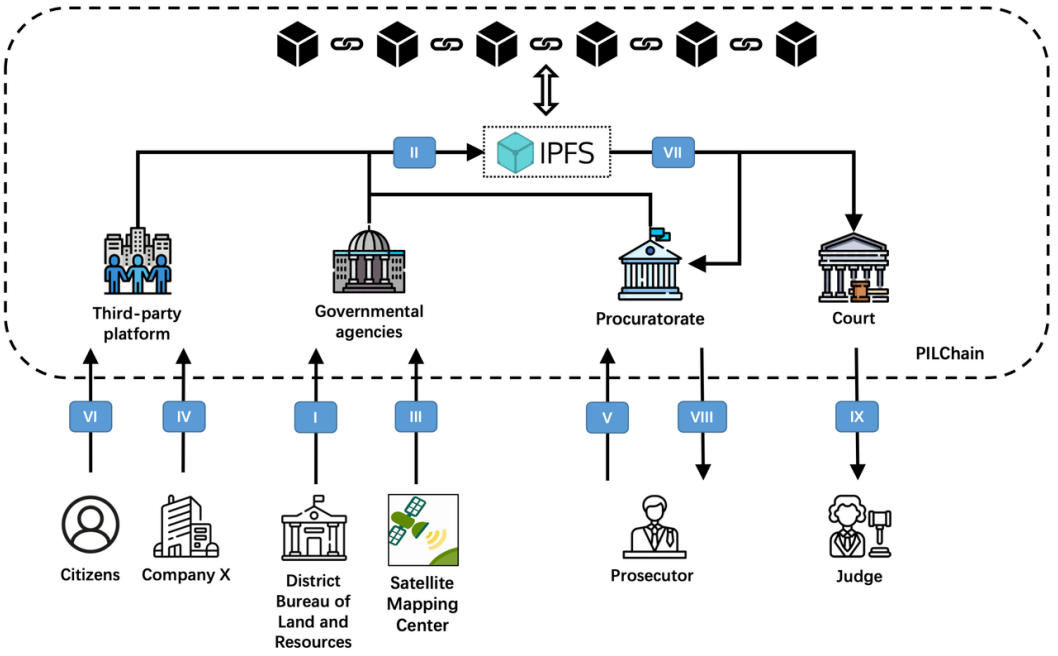
Permissions				
Roles	**Upload**	**Query**	**Access (own)**	**Access (other)**
Third-party platforms	√	√	√	
Governmental agencies	√	√	√	
Procuratorate	√	√	√	√
Court	√	√	√	√

from the blockchain and retrieves the encrypted evidence in the IPFS. For organizations that have no access to evidence data uploaded by others, the system compares the user's identifier with the *userID* in the composite primary key of the selected evidence. If it matches, it means that the evidence was uploaded by the evidence provider himself, and then the system retrieved the encrypted evidence in IPFS. Otherwise, the request is rejected. Next, the PILChain will perform another user verification by using the access control contract to obtain the decryption token *secrectToken* and decrypt the evidence. Even if the user bypasses the first access control by improper means, the access control requires user verification for obtaining a decryption token. Separating the acquisition of encrypted evidence and decryption of encrypted evidence into two steps, supplemented by two access controls, the PILChain further ensures the secure transmission of evidence data.

SCALABLE IMPLEMENTATION: A SCENARIO-BASED ILLUSTRATION

To show the implementation of the PILChain, the authors present an example scenario to visually demonstrate the workflow of the PILChain, as shown in Figure 6. The PILChain is used to support the evidence management of a real-world PIL case in Figure 1. This case involves six stakeholders: the procuratorate, the court, the District Bureau of Land and Resources, Company X, the Satellite Mapping Center, and local citizens. Details of the scenario are described below.

Figure 6. A scenario-based illustration of the PILChain



The key operations of evidence upload and evidence acquisition on the PILChain are illustrated as follows.

- **Evidence Upload:** All stakeholders involved in the case can upload and store relevant evidence through the PILChain with permission:
  - The District Bureau of Land and Resources, as a member of the governmental agencies organization, is required to upload the original document regarding the Administrative Penalty Decision and its proof of service.
  - The PILChain encrypts the original evidence locally and deposits it in IPFS, and then sends the IPFS link and the required token for decryption in the consortium blockchain.
  - The Satellite Mapping Center retrieves satellite remote sensing images of the cultivated land involved in the case at different time points and uploads the evidence through the governmental agencies organization. Then, go to Step 2.
  - Company X, with the help of the third-party platform organization, uploads the data required by the procuratorate in relation to the case, such as the parking lot construction plan. Then, go to Step 2.
  - The procuratorate conducts an investigation of Company X by inquiring managers and employees, and then uploads the investigation transcript. Then, go to Step 2.
  - With Identity Mixer in the PILChain, local citizens can also anonymously upload evidence about the destruction of farmland and the occupation of public habitat through the third-party platform organization. The evidence can be a photo of the site, a petition from a group of people, etc. Then, go to Step 2.
- **Evidence Acquisition:** According to the PILChain's access control protocol, only the procuratorate and the court can access the case evidence. Others can only access the evidence they have uploaded:

- After receiving a request for evidence access, the PILChain verifies the permissions of the organization to which it belongs. If the verification is passed, the IPFS link of the corresponding evidence and the token required for decryption will be queried on the consortium blockchain according to the request.
- The PILChain again verifies the identity of the evidence requester. For example, here, the prosecutor belongs to the procuratorate organization and has access to case evidence. Therefore, the PILChain will use the IPFS link to obtain the encrypted evidence, and then decrypt the evidence using the token. The prosecutor gets the original evidence he requested.
- Similarly, the court can repeat Steps 7 and 8 to directly access the original evidence for a PIL case, without having to wait for the evidence to be transferred between different agencies.

EVALUATION

Theoretical Analysis

This section discusses whether the proposed consortium blockchain-system model can solve the problems of secure data sharing and privacy protection in PIL practices. The security of the proposed system model will be analyzed in terms of access control, evidence confidentiality, evidence integrity, non-tamperability, traceability, and non-repudiation, privacy, and scalability.

Access Control: Different from the public chain, consortium blockchain only enables PIL stakeholders to access information, which ensures the security of judicial information. In addition, the system provides access control to further safeguard information security. Access control contracts deployed on blockchain regulate strict access to PIL evidence. All PIL stakeholders, including evidence providers and procuratorates, need to register in order to obtain identity credentials and private keys. CA assigns different authorities to different PIL stakeholders. For example, only the procuratorate and court can retrieve evidence upon request. Users who do not possess enough attributes required by access control cannot decrypt the cyphertext and access relevant information. Unauthorized access will be prevented.

Evidence Confidentiality

The PILChain encrypts evidence data locally, and then transfers the encrypted data to IPFS, which is a distributed file system for data storage and sharing. The IPFS address links and the token used for decryption are then transferred to the consortium blockchain. Evidence requesters need to pass two identity verifications to access evidence. Even if encrypted evidence is obtained from IPFS by improper means, the evidence cannot be viewed without a decryption token. This double insurance ensures the confidentiality of the evidence data in the transmission process.

Evidence Integrity and Non-Tamperability

The system not only guarantees the evidence confidentiality before the announcement, but also ensures the evidence integrity and non-tamperability with two non-tamperability mechanisms. First, CID is the unique fingerprint for encrypted evidence data in IPFS, which ensures data integrity, because any modification on original evidence data will lead to the change of CID. Second, the IPFS address link and decryption token, as well as the corresponding hash value, are stored in a block; the integrity can be verified by comparing the hash values.

Traceability and Non-Repudiation

The source of uploaded evidence can be traced because evidence-upload transactions include the evidence provider's signature. In addition, any operations on evidence data are recorded in blocks, which ensures evidence traceability. PIL stakeholders cannot deny the evidence operations.

Privacy: In addition to anonymity supported by blockchain, the PILChain enables evidence providers to selectively disclose personal information to the verifier through Identity Mixer with zero-knowledge techniques, and their privacy is protected to a great extent.

Scalability

On one hand, the system supports the storage and transfer of large evidence files at low latency. By combining IPFS and consortium blockchain, the proposed system maintains encrypted large-scale evidence files off-chain and stores small-size evidence information (e.g., IPFS address link, decryption token, etc.) on-chain. On the other hand, the system can be extended to include more data sources and judicial nodes. The system can also be connected to internal enterprise databases, administrative and law enforcement information platforms, social media platforms, and IoT devices (e.g., satellite remote sensing and environmental monitoring instruments) to obtain evidence data automatically. By including more judicial nodes, the evidence can be circulated within the judicial system for collaborative case handling. Regarding identity verification, the system can be connected to national identity information platforms and enterprise information databases to facilitate the identity verification of node users.

Experimental Evaluation

To further evaluate the PILChain, the authors built a prototype system based on Hyperledger Fabric. Apache JMeter was used to perform simulation and system analysis. The prototype system was evaluated in terms of widely used performance measures, including response time, latency, connection time, throughput, and transactions per second (TPS) (N. Gao et al., 2022; Ravi et al., 2022). JMeter is a Java-based load testing tool and can be used to measure the performance of both static and dynamic resources[3]. It can simulate load to a server, network, or object to test its overall performance.

Experiments were conducted on a cloud server with CentOS-G19z. The server has a 4-core CPU, runs on 4G RAM, and has 80G of system disk storage. The prototype of the PILChain was developed using Hyperledger Fabric 1.4.12, Docker 20.10.18, LevelDB database, and Go language. In the experiments, the authors created two organizations, one for uploading evidence and one for acquiring evidence, each with two peers. The orderer node provides ordering services based on Solo algorithm as the consensus.

To examine the impact of different volumes of evidence query requests on the load of the PILChain system, the authors simulated 50, 100, 150, 200, and 250 queries, respectively. The time granularity was set as one minute. JMeter records the changes in the system parameters and generates the corresponding test reports.

Table 2 provides a summary of the experimental results. Each row represents the system performance with different queries. *Execution* reports the number of Apache samples used for the experiment, and the number of failed samples in each execution. *Response time* is the average response time of the prototype system, while the *Latency* and *Connect time* refer to the average response latency and average connection time, respectively. The unit of time is milliseconds. *TPS* is the number of transactions that the system can process in a second, which is an important metric used to measure the processing power of the system. Bytes throughput reports the throughput of received and sent data per second.

As shown in Table 2, the number of samples with error is zero in all five experiments. As the number of queries grows, the average response time and latency change little, but the average connection time decreases, indicating that the system is relatively stable in performing evidence queries. TPS varies linearly, which illustrates the processing power of the PILChain in meeting the demand of many queries. Meanwhile, the overall level of system throughput increases steadily with the increase in query volume. This indicates that the system capacity of the PILChain is sufficient to cope with a large number of queries. Even if the queries in a short period of time bring a large amount of data, the system can adjust its capacity appropriately to guarantee data transmission.

Table 2. Summary of selected results of evidence query experiments

Requests	Executions	Avg. Response time (ms)	Avg. Latency (ms)	Avg. Connection time (ms)	TPS	Bytes Throughput (bytes/s)	
#Query	#Samples/ Fail					#Sent	#Received
50	250/0	5.18	5.14	0.088	4.17	629	525
100	500/0	5.01	4.96	0.052	8.33	1258	1050
150	750/0	4.79	4.76	0.036	12.50	1888	1575
200	1000/0	4.79	4.75	0.021	16.67	2517	2100
250	1250/0	5.30	5.27	0.017	20.83	3146	2625

In addition, the authors conducted a test on the process of evidence uploading with 50, 100, and 150 uploads separately. Table 3 provides the experimental results. The number of failed samples for all three experiments of evidence upload is zero. The operation of evidence upload packs the evidence information into blocks with a consensus mechanism, which explains that the response time during evidence upload is much higher than the query process. Overall, as the number of uploads grows, the response time, latency, TPS, and byte throughput of all three experiments are maintained at similar levels, but the average connection time decreases. This indicates that the PILChain is relatively stable in performing evidence uploads. The system can support stable uploads of a sufficient amount of evidence, and the upload latency of about two seconds is acceptable.

CONCLUSION AND DISCUSSIONS

This paper focuses on evidence sharing and privacy protection in PIL investigation. To solve the problems of insecure data sharing and identity disclosure during case investigation and evidence collection, the authors propose a consortium blockchain-system model for PIL practice, i.e., the PILChain. The PILChain combines blockchain technology with an off-chain storage system, which enables transmitting evidence efficiently over consortium blockchain with large-size evidence files. The permissioned consortium blockchain ensures secure data sharing between evidence providers and evidence requesters in PIL. First, citizens or companies can directly submit evidence to trusted third-party platforms through the PILChain that protects their privacy while verifying identity. They do not have to worry about their privacy being leaked when they disclose necessary information as required. Second, evidence can be securely uploaded by environmental protection authorities, procuratorates, public security organs, and on-site monitoring devices. The advantages of blockchain technology ensure the integrity, non-tamperability, traceability, and non-repudiation of uploaded evidence. Third,

Table 3. Summary of selected results of evidence upload experiments

Requests	Executions	Avg. Response time (ms)	Avg. Latency (ms)	Avg. Connection time (ms)	TPS	Bytes Throughput (bytes/s)	
#Upload	#Samples/ Fail					#Sent	#Received
50	250/0	2029.16	2030.50	0.12	2.09	600	277
100	500/0	2042.86	2034.50	0.13	2.08	600	277
150	750/0	2043.92	2042.67	0.06	2.09	600	277

prosecutors, judges, and other personnel can request access to evidence through the corresponding organizations in the PILChain with different permissions defined in access control, which guarantees the safety of evidence files. Last, the PILChain was implemented on Hyperledger Fabric to test its feasibility and efficiency. In summary, the PILChain supports the efficient transmission of large-size evidence files, provides fine-grained permissions for different PIL stakeholders, and protects the user privacy of evidence providers during case investigation by using a zero-knowledge identity proof.

Although the PILChain was designed for evidence investigation in PIL context, its key design can be extended to other types of litigation scenarios. We encourage future studies to explore additional litigation scenarios (e.g., criminal cases) to examine the generalizability of the PILChain. Besides, the data leakage attack was not considered in our solution. The leakage of gathered evidence will seriously affect the process of case investigation and the security of users. Last, in this paper, we only realized the PILChain prototype and demonstrated its feasibility. In the future, we need to further enhance its scalability by implementing it in real-world PIL investigations.

CONFLICT OF INTEREST

We have no known conflict of interest to disclose.

FUNDING INFORMATION

This work was supported by the National Natural Science Foundation of China (Grants No. 72271233, 71901208, and 71771212), the Fundamental Research Funds for the Central Universities and the Research Funds of Renmin University of China (No. 22XNA036), the Fundamental Research Funds for the Central Universities and the Scientific Research Innovation Project of China University of Political Science and Law (1000-10822507), and School of Interdisciplinary Studies, Renmin University of China.

AUTHOR NOTE

Correspondence concerning this article should be addressed to Corresponding author's name, University mailing address. Email: Corresponding author's email address.

REFERENCES

Agrawal, B., & Bhalotia, S. (2022). Witness protection scheme: India and United States. *Jus Corpus Law Journal*, *3*(1), 350–357.

Athanere, S., & Thakur, R. (2022). Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. *Journal of King Saud University-Computer and Information Sciences*, *34*(4), 1523–1534. doi:10.1016/j.jksuci.2022.01.019

Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. ArXiv Preprint ArXiv:1407.3561.

Billard, D. (2019). Blockchain-based digital evidence inventory. *Journal of Advances in Information Technology*, *10*(2), 41–47. doi:10.12720/jait.10.2.41-47

Casey, E. (2002). Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence*, *1*(2).

Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Science International: Digital Investigation, 35*, 301001. http://10.0.3.248/j.fsidi.2020.301001

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6–10), 71.

Debe, M., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2020). Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 20118–20128. doi:10.1109/ACCESS.2020.2968573

Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., & Werner, F. (2020). Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *International Journal of Production Research*, *58*(7), 2184–2199. doi:10.1080/00207543.2019.1627439

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems*, *42*(8), 1–11. doi:10.1007/s10916-018-0993-7 PMID:29931655

Gao, N., Han, D., Weng, T. H., Xia, B., Li, D., Castiglione, A., & Li, K. C. (2022). Modeling and analysis of port supply chain system based on Fabric blockchain. *Computers & Industrial Engineering*, *172*, 108527. doi:10.1016/j.cie.2022.108527

Gao, Y., Chen, Y., Lin, H., & Rodrigues, J. J. (2020, July). Blockchain based secure IoT data sharing framework for SDN-enabled smart communities. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 514–519). IEEE. doi:10.1109/INFOCOMWKSHPS50562.2020.9162725

Guo, J., Wei, X., Zhang, Y., Ma, J., Gao, H., Wang, L., & Liu, Z. (2022). Antitampering scheme of evidence transfer information in judicial system based on blockchain. *Security and Communication Networks*, *2022*, 2022. doi:10.1155/2022/5804109

Guo, S., Xiang, B., Xia, X., Yan, Z., & Li, Y. (2020). *Blockchain and federated learning based data security sharing mechanism over smart city*. Research Gate.

Härdle, W. K., Harvey, C. R., & Reule, R. C. G. (2020). Understanding cryptocurrencies. *Journal of Financial Econometrics*, *18*(2), 181–208. doi:10.1093/jjfinec/nbz033

Hegarty, R., Lamb, D. J., & Attwood, A. (2014, January). Digital Evidence Challenges in the Internet of Things. *INC* (pp. 163–172).

Holladay, Z. (2012). Public interest litigation in India as a paradigm for developing nations. *Indiana Journal of Global Legal Studies*, *19*(2), 555–573. doi:10.2979/indjglolegstu.19.2.555

Hurwitz, K. (2019). *Legal Remedies for Grand Corruption: The Role of Civil Society*. Open Society Justice Initiative.

Jain, S. R. (2022). Adoption of public interest litigation in diverse section. *Issue 2 Int'l JL Mgmt. &. Human.*, *5*, 622–633.

Javaid, U., Aman, M. N., & Sikdar, B. (2019, April). DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)* (pp. 1–5). IEEE.

Kim, D., Ihm, S. Y., & Son, Y. (2021). Two-level blockchain system for digital crime evidence management. *Sensors (Basel)*, *21*(9), 3051. doi:10.3390/s21093051 PMID:33925538

Li, M., Lal, C., Conti, M., & Hu, D. (2021). LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, *115*, 406–420. doi:10.1016/j.future.2020.09.038

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 1–5). IEEE. doi:10.1109/PIMRC.2017.8292361

Lin, S. Y., Zhang, L., Li, J., Ji, L. L., & Sun, Y. (2022). A survey of application research based on blockchain smart contract. *Wireless Networks*, *28*(2), 635–690. doi:10.1007/s11276-021-02874-x

Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 18207–18218. doi:10.1109/ACCESS.2020.2968492

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, *28*, 44–55. doi:10.1016/j.diin.2019.01.002

López-Aguilar, P., & Solanas, A. (2021, September). An effective approach to the cross-border exchange of digital evidence using blockchain. In *Applications in Electronics Pervading Industry, Environment and Society* (pp. 132–138). Springer International Publishing.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, *88*, 101653. doi:10.1016/j.cose.2019.101653

Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., & Ylianttila, M. (2019, May). Blockchain based proxy re-encryption scheme for secure IoT data sharing. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 99–103). IEEE. doi:10.1109/BLOC.2019.8751336

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. doi:10.1007/s12599-017-0467-3

Oatley, G. C. (2022). Themes in data mining, big data, and crime analytics. *Wiley Interdisciplinary Reviews. Data Mining and Knowledge Discovery*, *12*(2), e1432. doi:10.1002/widm.1432

Paraschiv, D. S. (2011). Public interest litigation in Europe. *Contemporary Readings in Law and Social Justice*, *3*(1), 122–127.

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, *25*(4), 1398–1411. doi:10.1177/1460458218769699 PMID:29692204

Philip, A. O., & Saravanaguru, R. A. K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 4031–4046. doi:10.1016/j.jksuci.2022.06.001

Rahman, M. U., Baiardi, F., & Ricci, L. (2020, December). Blockchain smart contract for scalable data sharing in IoT: a case study of smart agriculture. In *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)* (pp. 1–7). IEEE. doi:10.1109/GCAIoT51063.2020.9345874

Ravi, D., Ramachandran, S., Vignesh, R., Falmari, V. R., & Brindha, M. (2022). Privacy preserving transparent supply chain management through Hyperledger Fabric. *Blockchain: Research and Applications*, *3*(2), 100072.

Samuels, H. (2018). Public interest litigation and the civil society factor. *Legal Studies. The Journal of the Society of Legal Scholars.*, *38*(4), 515–528. https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.legstd38.34&lang=zh-cn&site=eds-live

Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. *Applied Sciences (Basel, Switzerland)*, *9*(6), 1207. doi:10.3390/app9061207

Sirui, C., & Zhihui, L. (2015). A reference-oriented study of the legal system of food safety risk communication. *China Legal Science*, *3*(3), 94–117.

Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., & Javaid, N. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Applied Sciences (Basel, Switzerland)*, *10*(2), 488. doi:10.3390/app10020488

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Report*, *26*(3), 304–308. doi:10.1016/j.clsr.2010.03.002

Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, *491*, 151–165. doi:10.1016/j.ins.2019.04.011

Tsai, F. C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, *192*, 2779–2788. doi:10.1016/j.procs.2021.09.048

Verma, A., Bhattacharya, P., Saraswat, D., & Tanwar, S. (2021). NyaYa: Blockchain-based electronic law record management scheme for judicial investigations. *Journal of Information Security and Applications*, *63*, 103025. doi:10.1016/j.jisa.2021.103025

Wang, A. L., & Gao, J. (2010). Environmental courts and the development of environmental public interest litigation in China. *J. Ct. Innovation*, *3*, 37.

Wang, Y., Ji, R., & Peng, Y. (2022). Research on legal protection of consumers' personal information from the perspective of public interest litigation. *Asian Journal of Social Science Studies*, *7*(4), 38. doi:10.20849/ajsss.v7i4.1088

Wang, Y., & Xia, Y. (2023). Judicializing environmental politics? China's procurator-led public interest litigation against the government. *The China Quarterly*, *253*, 90–106. doi:10.1017/S0305741022001709

Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 36*, 105401. http://10.0.3.248/j.clsr.2020.105401

Xie, L., & Xu, L. (2022). Environmental public interest litigation in china: Findings from 570 court cases brought by NGOs, public prosecutors and local government. *Journal of Environmental Law*, *34*(1), 53–81. https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.jenv34.5&lang=zh-cn&site=eds-live. doi:10.1093/jel/eqab029

Xu, S., Cai, X., Zhao, Y., Ren, Z., Du, L., Wang, Q., & Zhou, J. (2022). zkrpChain: Towards multi-party privacy-preserving data auditing for consortium blockchains based on zero-knowledge range proofs. *Future Generation Computer Systems*, *128*, 490–504. doi:10.1016/j.future.2021.09.034

Yan, W. (2021). The Zhenhua case: The emergence of civil environmental public interest litigation in China. *Journal of World Energy Law and Business*, *14*(2), 116–128. https://search.ebscohost.com/login.aspx?direct=true&db=edswst&AN=edswst.2564971&lang=zh-cn&site=eds-live. doi:10.1093/jwelb/jwab008

Yan, W., Shen, J., Cao, Z., & Dong, X. (2020, March). Blockchain based digital evidence chain of custody. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology* (pp. 19–23). IEEE. doi:10.1145/3390566.3391690

Yap, P. J., & Lau, H. (Eds.). (2011). *Public interest litigation in Asia*. Routledge.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLoS One*, *11*(10), e0163477. doi:10.1371/journal.pone.0163477 PMID:27695049

Zaghloul, E., Li, T., & Ren, J. (2019, February). Security and privacy of electronic health records: decentralized and hierarchical data sharing using smart contracts. In *2019 International Conference on Computing, Networking and Communications (ICNC)* (pp. 375–379). IEEE. doi:10.1109/ICCNC.2019.8685552

Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, *42*(8), 1–18. doi:10.1007/s10916-018-0995-5 PMID:29956061

Zhang, W., Wei, C. P., Jiang, Q., Peng, C. H., & Zhao, J. L. (2021). Beyond the block: A novel blockchain-based technical model for long-term care insurance. *Journal of Management Information Systems*, *38*(2), 374–400. doi:10.1080/07421222.2021.1912926

Zheng, B. K., Zhu, L. H., Shen, M., Gao, F., Zhang, C., Li, Y. D., & Yang, J. (2018). Scalable and privacy-preserving data sharing based on blockchain. *Journal of Computer Science and Technology*, *33*(3), 557–567. doi:10.1007/s11390-018-1840-5

Zhu, X., Qiu, T., & Liu, D. (2023). Resisting public monitoring in authoritarian regimes: Evidence from local environmental litigation in China. *Governance: An International Journal of Policy, Administration and Institutions*, *36*(2), 459–477. doi:10.1111/gove.12675

Zhuang, H., & Wolf, S. A. (2021). Environmental public interest litigation: New roles for civil society organizations in environmental governance in China. *Environmental Sociology*, *7*(4), 393–406. doi:10.1080/23251042.2021.1897243

ENDNOTES

[1] https://www.spp.gov.cn/xwfbh/wsfbt/202206/t20220630_561637.shtml#1
[2] https://www.investopedia.com/news/uk-courts-start-pilot-blockchain-evidence-system/
[3] https://jmeter.apache.org/