Computers and Electrical Engineering 100 (2022) 108027

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A decentralized autonomous personal data management system in banking sector

Dr. M Anna Gustina Zainal [a], Ricardo Fernando Cosio Borda [b], Yousef Methkal Abd Algani [c], Mr. Bhaskarrao Yakkala [d], Dr. S Sanjith [e], Iskandar Muda [f], T. Kalaichelvi [g], M. Mahendran [h], B. Kiran Bala [i]

[a] *Doctor of Communication, Department of Communication, University of Lampung, Indonesia*
[b] *Universidad Autónoma del Perú*
[c] *Department of Mathematics, Sakhnin College, Israel.Department of Mathematics, The Arab Academic College for Education in Israel-Haifa, Israel*
[d] *Assistant Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai, India*
[e] *Assistant Professor & Head, Department of Computer Science, St. Alphonsa College of Arts and Science, Soosaipuram, Karinkal, Kanyakumari District, Tamilnadu, 629157, India*
[f] *Professor, Department of Doctoral Program, Faculty Economic and Business, Universitas Sumatera Utara, Medan, Indonesia, 20222Jl. Prof TM Hanafiah 12, USU Campus, Padang bulan, Medan, Indonesia*
[g] *HoD, Department of Artificial Intelligence and Data Science, Panimalar Institute of Technology, Tamil Nadu, India*
[h] *Department of CSE, Panimalar Engineering College, Chennai, India*
[i] *HoD, Department of Artificial Intelligence and Data Science, K.Ramakrishnan College of Engineering, Trichy, Tamil Nadu, India*

ARTICLE INFO

Keywords:
Blockchain
Bitcoin
Personal data
Privacy
Security

ABSTRACT

The present security systems encounter vulnerable surveillance and protection breaches in financial domains day by day. These systems compromise the privacy of the users in such a way that their personal data are collected and controlled by the third-parties. In this regard, Bitcoin has been implemented in the financial space. It has made possible the trusted and auditable computing via decentralized network associated with a public ledger. This work proposes a decentralized personal data management system for banking sector using block chain which makes sure that the user can control their personal data in their own .It presents a Privacy-Protected Blockchain network in which all data is encoded within a controlled time period. Despite the fact that the data is available in the past, this design can successfully preserve user privacy and protect from deceivers, providing the data more stable and healthier. Blockchain has its advantages over features such as transparency, decentralization and immutability. In the proposed model, a protocol is implemented which converts the blockchain into automated access control manager. There is no need for a third party to be trusted for the implementation of this model. In the proposed system, the transactions are not limited to financial transactions like Bitcoin, it also includes data storing, sharing and querying. Hence, the use of blockchain could reduce the overly concern about securing and compartmentalizing the data.

1. Introduction

The storage of data is increasing rapidly in today's world. The data stored are the valuable asset for today's economy. In the era of

E-mail addresses: anna.gustina@fisip.unila.ac.id (Dr.M. Anna Gustina Zainal), bhaskarrao@saveetha.com (Mr.B. Yakkala).

https://doi.org/10.1016/j.compeleceng.2022.108027
Received 18 November 2021; Received in revised form 15 April 2022; Accepted 19 April 2022

Big Data, the data has been collected and stored continuously. These data are analyzed for several innovative processes. The data collected from organizations can be used to foresee the future trends byoptimizing the services and decision-making processes.

E-commerce applications dependmostly on third-party financial services for processing online transactions. Although these services do their work well, there existstill some weaknesses in its trust. The reason is that the complete irreversible transactions are impossible due to the fact that mediating disputes cannot be avoided by financial organizations. The mediation cost increases the transaction costs, reduces the minimum transaction size,haltssmall casual transactions and high cost is required in making irreversible transactions. Also, it is misused by some frauds. These limitations can be avoided by using physical currencies. There are no such systems for making online transactions without trusted parties [1].Bitcoin is a protocol for online communication which makes use of virtual currencies. The rules followed in Bitcoinare framed by Engineers without the intervention of regulators or lawyers. The transactions made using bitcoin were stored in a log distributed over the network of participants instead of storing it in a single or a set of servers. The bitcoin account can be created by anyone with no additional charges, no centralized vetting process and without the need of their original name [2].The aim of introducing the Bitcoin is to provide a secure alternate currency for financial infrastructure all over the world. The bitcoin resists regulation and promotes anonymity [3].

Recently, the blockchain grabs the attention of the several stakeholders across the fields like finance, healthcare, government sectors, real estates and utilities. The reason behind the growth of blockchain in such fields is due to the decentralization of transactions and storages without any trusted intermediaries or central authorities but it can certainlyattain similar functions [4]. In this data driven culture, the concern for the privacy and security of users' data is increasing. Large number of data was collected from a user by the centralized public and private organizations. None of those data could be controlled by the users, even they were unaware of what data had been used for what purpose. There are numerous methods available to preserve the privacy and security from technological as well as from legislative views [5].By analyzing the social media of an individual, their identity and day-to-day activities, online and professional life can also be identified [6].The wide range of using web services and smartphones collects large number of personal metadata of an individual which includes their web-search, call logs, location, etc. These data are being used by big-data researchers and by several organizations. The lack of technical solutions in managing the metadata makes the data to be shared without the control of the particular individual. Hence, the individuals have no knowledge about the risks caused by collection and the usage of the metadata [7].

The growth in data availability and the advancement in artificial intelligence provide us with some unique prospects in the field of healthcare along with several challenges for the patients, regulators, providers and the developers. The recent deep learning and transfer learning approaches turns an individual's data into powerful data sources for the purpose of predictive analysis. Till now, the patients are unaware of the exact value of their data.Further, they alsohave no access control over their medical records [8]. Medical records need a lot of improvement. The medical data of patients are stored by variousauthorities and the said data has been transferred from one storage space to another's storage space. This transfer leads to loss of access to the data by the patients.But the data providers can easily get access over it [9].The application of Electronic Medical Records (EMR)in the enhancement of healthcare intelligence is viewed as a serious task. The challenges associated with handling the medical data are, collecting, storing and analyzing them without violating the privacy. Subjective researches revealed that the lack of proper security features leads to several data breaches, exposing the patients to social stigma, mental anguish and economic threats [10].

The blockchain is now in trend due to the popularity and success of bitcoin. It can be clearly viewed by the growth in the usage of blockchain technology in several fields. This rapid growth is due to its transparency in data sharing and usage. The blockchain is found to be highly secured, as all the transactions were recorded on the chain which expands continuously which makes the modification or deletion of a block as highly challenging [11]. Till now, data sharing is an irreversible processthat is reversing the sent data or limiting its usage after deliverybecomes really impossible. However, giving permission to access the data can be a reversible and controllable. This is because, the raw data can only be seen by the owner of the data.Apart from them, no one can access it. This fact can change the current data analysis processes [12]. The lives of humans are being digitalized and thereby leaving traces of personal data behind. Presently, some of the larger multinational companies provide many services for getting profit via lending the user's data for payment. The users can get better services through data analytics, but their control over their personal data gets diminished [13].

The blockchain technology makes use of several decentralized applications, instead of depending on the trusted intermediary which depends on a trustless environment. It is believed that blockchain can resolve the challenges in managing the personal data of users [14]. Several user-centric services collect the personal data of users like age, race, location, driving license details, security numbers etc. Half of the population uses social networking platforms which gathera greater number of personal data from each and every user. For premium apps or sites, users need to register in it on the other hand, for free services, the user's identity has been traded to get profit [15].Not only for Bitcoins, the blockchain is now extensively used in several other applications related to transactions, machine to machine and human to human communications. Blockchainin various applications are used because of its privacy, security, traceability, inherent data provenance and time stamping nature.Blockchain seems to be well suited for the developing countries considering the trust as a main concern [16].Here, the securities exchange is now digitalized and hence, the data security is an important apprehension. The securities exchange is the place where trading shares of bonds and stock happens [17].In the field of Human Resource Management (HRM), applying Information Technology (IT) is essential so as to effectively implement Industry 4.0. A secure, transparent, efficient and non-biased environment has been achieved by using the HRM system when it is associated with IT. This can be possible by applying Blockchain technology which works through a distributed ledger system [18].

To address the conflict between the user's strong need for individual privacy and the typical blockchain system's publication of all information, the privacy-protected Blockchain Network introduces a new function. This new application allows the user to configure the system's encryption duration. As a result, people involved in the transaction can reach an agreement on appropriate encryption duration. This meets the user's requirement for personal privacy quite effectively. In Bigdata analytics, cloud computing is considered

to be the most promising platform due to its scalability, provisioning and advanced computing ability. The concern is with the data collected by the cloud service providers. Large quantity of data had been gathered by cloud service providers like contact details, credit card and back account details, etc. In addition to this, loyalty reward card proliferation also tracks the purchase patterns of users by retailers and stores them on cloud platform [19].The results indicate that the proposed study has successfully fulfilled 20% of a redaction time comparison to prior privacy-preserving blockchains, having resulted in higher redaction efficiency. Blockchain records the history of all the transactions on a shared ledger. Starting from Bitcoin, blockchain as an immutable and consistent system, is now applied over several other areas for storing the transactions and data in a highly secured and controlled manner [20].

In this study, a privacy preserving blockchain and off-blockchain personal data management system has been introduced. This paper is organized as related works in section II, problem statement and solution in section III, proposed methodology in section IV followed by result and discussion in section V and finally concluded in section VI.

2. Related work

The problem of double-spending can be prevented via peer-to-peer network, the transactions were timestamped by a hash-based proof of work and it cannot be modified without performing the proof of work again. The rules followed in bitcoin account are highly flexible, private and not as much amenable to regulatory oversight than other payment platforms [2].A survey on the success of bitcoin applications and the criminal activities on bitcoin like dark market, malware, online extortion and theft and the solutions made for solving such activities has been described in [3].

The use of blockchain in Internet of Things has been analyzed and reviewed the working of it on smart contracts. Also, the suggestion to solve the issues faced during the deployment has alsobeen described [4]. An auditing system for analyzing the data usage based on blockchain technology is given in the existing works [5]. This system depends on 3 types of units namely, data owner, data controller as Service Provider (SP) and data processor as Service Controller. The data owner subscribes to the data controller SP for a contract of data usage. The data owner is the only person who can specify the policies for the transmission of data from owner to data controller SP. The data controller SP creates a new smart contract and is notified to the data owner of the usage policy has been afforded.Research on the online identity of a user has been performed by gathering valuable information from several different online sources using a new method called Tsinghua University User Reputation System (TURS) [6]. This method makes use of the gathered information to calculate the user's online, personality and professional rating. The ratings of online reputation provided will be based on the number of followers, comments/likes/tags, votes by the user, tweets, friends added and the views they got per month.

A technique called OpenPDS which is actually a field-tested Personal Data Store has been introduced to allow the users to collect, store and provide access to the third parties. Also, a question-and-answer scheme is introduced so as to provide a practical method of privacy protection of metadata. A review on artificial intelligence and deep learning, based on biomedical research tools has been performed [8]. Then, a Highly Distributed Storage System (HDSS) concept has been discussed. It uses Exonum, an open-source framework of blockchain to analyze its use in healthcare.Here, the users can ensure that they have the control over their data, have the ability to provide access to anyone and can gain profit with it. MedRec, a blockchain-based Electronic Medical Data management system has been demonstrated [9]. This system can manage authenticity, accountability, confidentiality and sharing of sensitive data. The medical stakeholders were invited as miners to attain patient data as mining rewards through Proof-of-Work.

A mobile application named Healthcare Data Gateway that works on the basis of blockchain has been introduced so as to make the patients to own, share and control their data.To easily organize various personal medical information, a unified Indicator Centric Schema (ICS) has been used. The author also suggests that Multi Party Computation (MPC) can provide an untrusted third party to compute patient's data with no privacy violation.A model that pursues mitigating lack of control over blockchain named as Controllable Blockchain Data Management (CBDM) has been proposed [11]. A node called Trust Authority has been introduced to provide authorization to high level voting, when it is compared with other nodes. The veto power involved in this system prevents malicious voting. In this system, only the metadata are stored in cloud so as to improve the efficiency of block construction and eliminating the distributive storage wastes.A computational model named Enigma has been introduced [12], which is a decentralized platform that guarantees privacy of user data. Enigma works on the basis of an optimized secure MPC provided by a verifiable secret sharing system. The data are stored in a modified distributed hashtable. An external blockchain has been used to control the network. Same as Bitcoin, Enigma also eliminates the use of third parties and enables autonomous of personal data control.

A system of personal data and identity management based on Blockchain, BPDIMS has been demonstrated so as to enable high-level security, transparency and trust in managing the personal data. This system is a human centric and GDPR compliant model based on blockchain. A blockchain based proof of permission protocol has been designed to reduce the fictions occurred in the existing personal data management approaches. These fictions are theoretically achievable, but practically it is impossible due to the limitations found in blockchain technology and smart contracts. Also in this paper, a medical data sharing has been implemented so as to determine the efficiency and feasibility of this system. The Article 42 and Article25 of General Data Protection Regulation (GDPR) demands the right to forget and right to erase the data. However, these rights are completely against the immutable feature of blockchain. Hence, a GDPR Decentralized Personal Identifiable Information Sharing Scheme has been introduced [15]. This system can facilitate data sharing, tracking, modifying and even deleting.

The summary of many literatures that describes the application of blockchain and other digital ledger methodologies in different fields beyond crypto currencies has been given in [16]. This survey is made to provide proper conclusion for all the challenges faced in the existing systems to facilitate effective use of blockchain technology in future, other than in the field of crypto currency. Blockchain is considered to be a Trust Machine to store the transactions of stock exchanges securely, based on technological and legal factors provided by the particular country.A Blockchain based Recruitment Management System (BcRMS) and Human Resource Management

Table 1
Types of Blockchain node.

Type of Node	Function	Examples
Full Node	Preserve a complete copy of the blockchain, Produce blocks, Authorize blocks, Authorize Transactions, Produce a new broadcast and transaction.	Servers or desktop computers with adequate hardware resources
Half Node	Only keep a limited copy of the blockchain, Authorize blocks, Authorize Transactions, Old records should be validated as peer support. Produce a new broadcast and transaction.	Laptops or alike
Simple Node	Authorize a new transaction, Produce a new broadcast and transaction.	Limited capacity of mobile devices or Internet of Things (IoT)

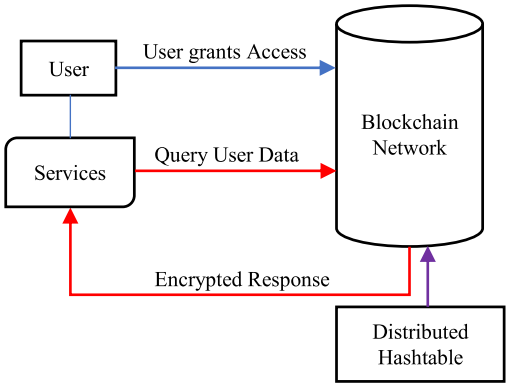

Fig. 1. Proposed Decentralized Data Management System.

System (BcHRMS) has been introduced for Industry 4.0.The results obtained from this system proved that it has certainmeritsover the existing recruitment and HRM systems.To semi-automate the knowledge extraction as RDF tuples from privacy documents, techniques such as Semantic Web, Natural Language Processing and Text Mininghave been used. The key information and control that are to be included in privacy policy has been identified by a technique called CMU Link Parser to outline the ontology to signify them. This semantic framework has been build using a three-phase approach which includes, ontology development, extraction of terms and definitions and analyzingthe permissions and obligations.A Hyperledger Fabric that supports private data by using an on-chain secure MPC protocols has been demonstrated in [20]. A demo auction application has been implemented and tested using this architecture. The results showed that this system has further improvement on adding two components to execute the smart contract based on private data.

3. Problem statement and solution

Several researches have been studied their detailed description on blockchain and its applications over personal data management have been implemented using various methodologies which were studied in previous sections [21]. In this paper, the privacy problems related to the use of third-party services has been addressed, particularly for mobile platforms. The reason for focusing on mobile platforms is that they often collect personal data from the users without their control.

The proposed system can also be used to share the medical data of patients for research purposes. The patients can have the ability to monitor how their data has been used by researchers.They can also to opt-out instantly, if they are not interested in sharing their personal medical information [22]. The persons themselves are considered as the owner of the data and have full control to how such data can be used. The services are considered as the guests after getting permission from the owners.

Most of the mobile applications ask for a set of access permissions while signing up into it. There is no way to alter those permissions. The only way is to opt-out from it. The proposed system grants access to alter such permissions and to revoke the access of previously shared data. This system improves the permissions of mobile applications, keeping the user interface to be constant and storing the access control policies safely in the blockchain being accessed only by the users.

4. Proposed methodlolgy

The proposed model is comprised of three entities namely Smartphone Users, Services and the Nodes.These nodes can function as

Table 2
Comparison of security services.

	Central Database	Distributed Database	Blockchain
Reliability	Low	Average	High
Integrity	Average	Average	High
Privacy	High	Average	Variable
Fault detection	Low	High	High

clients and servers at the very same time, resulting a decentralized system [23]. Table 1 summarizes the functions that nodes with physical devices can have. These nodes employ consensus algorithm to reach a consensus on operations, including who should write the next block. The based on limited writes the new block, which is then disseminated to all neighbors.The smartphone users who have more interest to download and use mobile applications have been selected. The services means, the personalized service and target ad providers who collect the personal data for processing the business and operational services has been selected. The Nodes means, the trusted entities that maintains blockchain and distributed private key that has been stored in return for incentive. In blockchain, a user can be completely anonymous. In this case, the service profiles of the used would be stored and verified for identity.

Fig. 1 shows that the architecture of Proposed Decentralized data is a management system. Two types of transactions are being accepted by blockchain [24]. One is for access control management and the other is for strong and retrieving of data. These two operations are programmed into the mobile Software development Kit for further use in the process of developing the mobile application.

The proposed system of decentralized personal data management works as follows: First,a user should install the mobile application in his/hersmartphone. Then, they should sign up into it. After their first sign up, a new shared user-service identity has been generated and transferred to the blockchain via user-blockchain transaction, along with its related permissions.The sensor data has been collected from the smartphone are encrypted by shared encryption key. This data is transferred to the blockchain via service-blockchain transaction which is then sent to an Off-Blockchain Key-value storage system. Here, only the pointer named as SHA-256 hash value of data has been retained in the public ledger. Now, the user and the service can query the data using its key. Then, the digital signature is verified by the blockchain, whether it is from user or service. If the digital signature is from service, then the data access permission is also being verified. The granted permission in a user-blockchain transaction can be modified or revoked by the user at any time by creating a new set of permission.The off-blockchain storage is an execution ofDistributed HashTable (DHT). The DHT is upheld by a network containing nodes that satisfies the specified transaction. All the data are completely randomized over the nodes and simulated to make sure its availability.

The network protocol used in the proposed system is the standard cryptographic building block.The symmetric encryption has been given by three tuples that includes the generator algorithm, the encryption algorithm and the decryption algorithm. The digital signature has been given by three tuples that includes the generator algorithm, the signature algorithm and the verification algorithm that follows the implementation of Elliptic Curve Digital Signature (ECDSA) with secp256k1 curve and cryptographic hash function, implemented by the instance of SHA-256 algorithm.

4.1. Buillding blocks

The building block used in the proposed system is as follows:

Identities:Usually, blockchain makes use of pseudo identity method. The user has the ability togenerate many public keys they need to enhance the privacy of their data. In the proposed decentralized system, compound identity mechanism is employed. It is a form of shared identity method, in which some parites own the identity like owner and the remaining will have restricted access like guests.

Blockchain Memory: Consider the blockchain memory as L, then hashtable as L: $\{0, 1\}^{256} \rightarrow \{0, 1\}^{N}$, which has the ability to store larger documents. It is assumed to be tamper proof under the blockchain based adversarial model. The blockchain is made of a sequence of time-stamped transactions with various output addresses having each of size 160-bit. In the blockchain memory space, first 2 outputs of a transaction encode are 256-bit memory address pointer and some auxiliaries are from metadata. All the remaining output forms a serialized document.

Policy: The policy is a set of permissions that a user provides to a service. When a smart phone application is installed by a user that requires permission for accessing the location and contacts, then the policy can be denoted as {*location, contacts*}. By this way, all the information has been securely stored. In any of the cases, when occurs a cheat, it can be easily identified by the user, as they can view each and find any modification happening with their data.

Auxiliary Functitons: The messages sent via transaction are deserializedby *Parse*(x)and checks whether the creator have all the proper permissions using the *CheckPolicy*.

4.2. Privacy and security analysis

The proposed decentralized personal data management system allows only the user to have control their data. The digital signature provided on the transactions makes sure that an adversary can't act like the user or can involve in network corruption. If they do so, it is considered as a forged or gaining control on many resources of the network. In public ledger, there will be hashed pointers only and

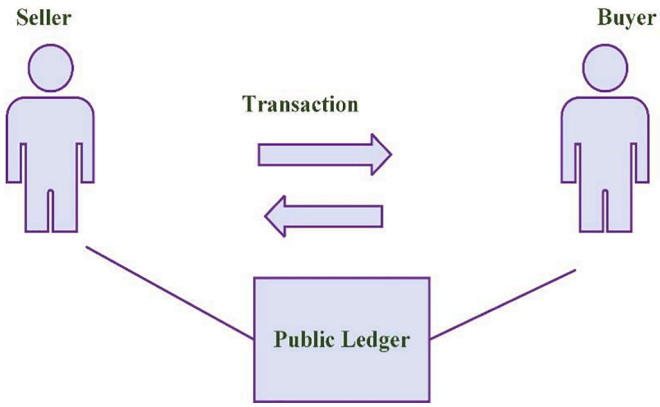

Fig. 2. Ledger.

hence the adversary can't learn whatever in it. If one or more distributions are stable by an adversary, then they can't observe what is in the raw data.As it has been encrypted by a key, it will not be same as that of any nodes.In the new generation, compound identity ensures that only a little data has been compromised while the adversary gets the signing and encryption keys. Here, the data will be secure if the adversary gets only one of the keys. The identities can be split further so as itreduces the exposure of one compound identity.

Table 2 compares the security services offered by blockchains, central databases, and distributed databases. Block chain technology is ideal for providing data integrity, reliability, and fault detection services.

4.3. Bitcoin

Bitcoinwas invented in 2008 as a new means to send value over the internet. Bitcoin was invented by Vitalik Buterin, a developer. Bitcoin is a type of digital currency that is created and stored electronically. It runs as a decentralized application. This has direct control over the exchange of virtual currency. Bitcoin's value has risen in the last year. One of the primary problems that Bitcoin seeks to solve is the decentralized monitoring and verification of transactions. It will save the entire transaction history. Blockchain was created primarily to facilitate the exchange of this virtual currency. If the consumer wants the most historical development, the selection is challenging .Therefore conducting a deal, the regulations and restrictions will be laid down in the form of a shared ledger. Transactions are only possible between two people, and the sender must enter an electronic sign before proceeding. This digital sign validates the transaction. If this sign is validated, the transaction will proceed, implying that bitcoin will be exchanged.

In blockchain, a ledger is a decentralized program assigned to each user. When a transaction is completed, it is automatically entered in the ledger. For example, in Fig. 2, suppose there are two people, A and B. Person A offers100 rupees to person B. This blockchain provides another person. They usually have their own ledger. This information will be updated immediately in everybody's ledger. Person A stated that he should only pay B ten rupees. Then there will be a voting system. This voting system can demonstrate that person A's assertion is not valid. As a result, it will be refused.

4.4. Privacy-Protected blockchain network

This made certain adjustments to the standard blockchain smart contract framework in order to make it healthier. The standard transaction procedure in the Privacy-Protected Blockchain System is separated into three sections, as illustrated in Fig. 3.

- The user determines which users have authorization to change the data set and how long the encrypted will last. The users then utilize a smart contract to submit their data and deposit it on the server. The smart contract management server creates a data set from the data marked with the uploader's ID. The data set is subsequently encrypted and distributed to all individuals involved in the transaction. In this manner, all necessary data is captured on the servers.
- A user with authority to modify a data set works on a data set via a smart contract, but the user can only provide a lawful operation command to the servers via the smart contract and cannot directly alter or see the precise data into data set.
- When the predefined encryption length expires and the anonymity of the set of data is no longer relevant, the blockchain network will distribute the decryption to all articles were analyzed. At this point, any user can see all of the data from the data set. When all users agree that the transaction was successful, the user's contribution will be allocated to the user in accordance with the allocation criteria.

The major element of a privacy-protected Blockchain System is that all data is encrypted in a brief period of time, yet all data is public in the past. As a result, when the transactions must remain secret, the smart contract will not communicate the private keys to the user, keeping the transaction contents secure and private. When the privacy of the transaction content is no longer necessary after a

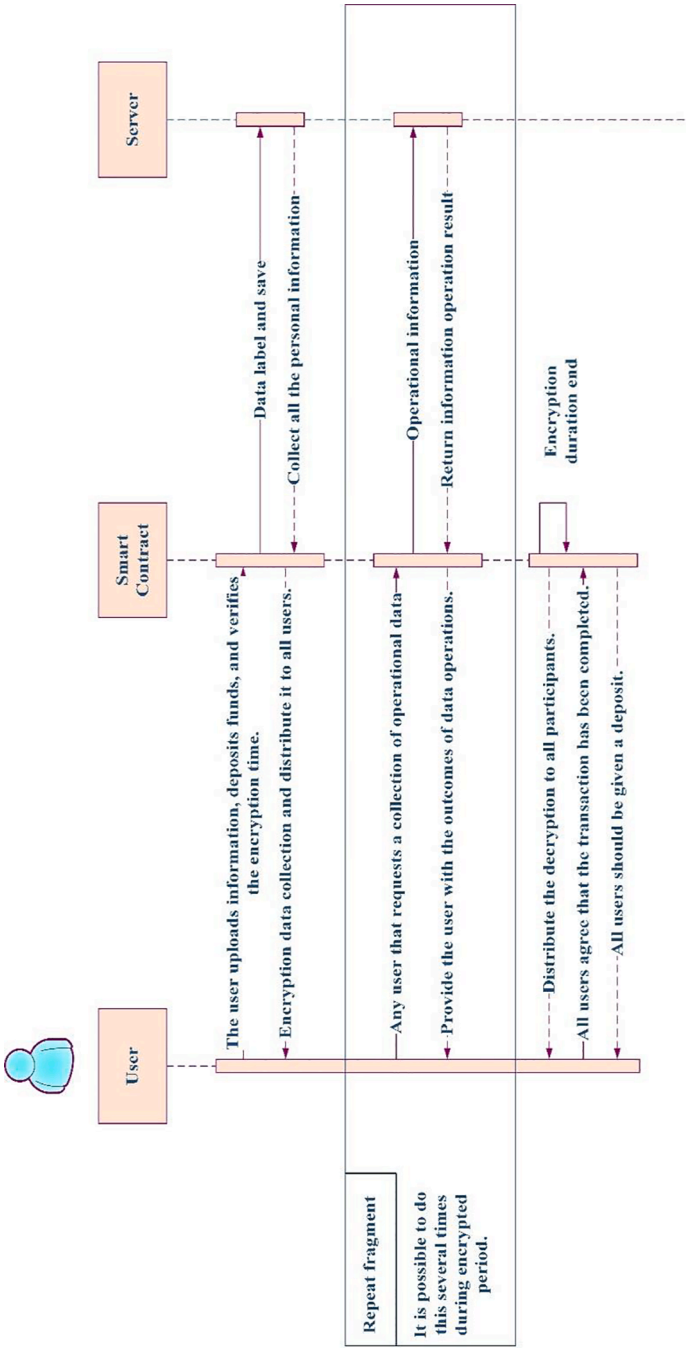

Fig. 3. Diagram of a Health Trading Process in a Privacy-Protected Blockchain Network.

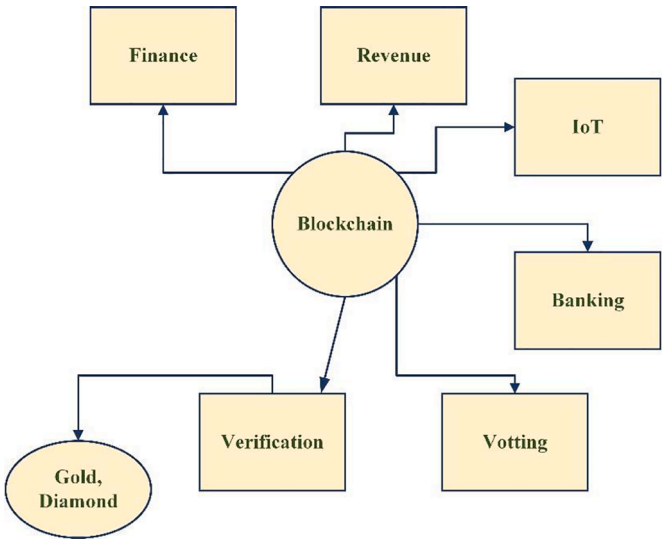

Fig. 4. Blockchain Application.

time of trade, the smart contract will disclose the decryption key with all participating users. When the user obtains the key and releases the encrypted information set in a transfer without a deceiver, the smart deal's work is completed.

However, if there is indeed a liar in this deal, it will make a significant difference. The involvement of deceivers can be detrimental to honest participants. After getting the key, honest participants will be able to see all of the data in the data set. In addition, the material is labelledwith the uploader's ID. Honest individuals can quickly identify the deceiver's ID for tagging it on the bogus data. At this moment, the smart contract will take action, imposing sufficient punishment on the deceiver in accordance with the established method, and punishing the deceive again for money acquired to compensate the harmed honest participant.

When the deceiver is doomed to be caught and punished, the high likelihood of judgment and severe punishments significantly raise the illegal price of the deceiver. As the high penalty of crime reduces the likelihood of deceivers, the institution becomes stronger and much more stable.

4.5. Blockchain application

Blockchain has a wide range of industrial uses. Some examples are provided below Fig. 4. Today, banking executives are attempting to adapt blockchain in order to conduct secure transactions. Finance is among the most visible use of blockchain technology.

5. ResultS and future recommendations

This section focused on a basic development of the Privacy-Protected Blockchain Network and a trade scenario study.

1 Privacy-protected Blockchain system

The system is made up of one ordered node, three Zookeeper nodes, four Kafka brokers, and four peer nodes. Organization 1 owns two of the peer nodes, whereas Organization 2 owns the other two. We updated the function invoke and so when clients use it in a privacy-protected bitcoinblockchain, the ciphertext of the transaction is sent to all users in the system. The transaction information is encrypted using DES encryption. After 20 s, all users are given a key that will allow them to decrypt the cipher - text. At this stage, the user can decrypt the ciphertext and acquire transaction content data.

1 Experiment with a (k, n) threshold to simulate a trading situation

They devised an experiment to imitate a trade scenario in order to validate the system security of the Privacy-Protected Public Blockchain and also to evaluate the defenses against the deceiver. In the experiment, the Shamir Threshold Approach [24] has been utilized, and the encryption technique is known as (k, n) Threshold. It splits the secret into n duplicates and necessitates the collaboration of at least k secret owners in order to restore the knowledge.

Steps for experiment:

- Using the ShamirThreshold Approach, divide the secret K into 85 subkeys, and any five accurate subkeys can reconstitute the secret.

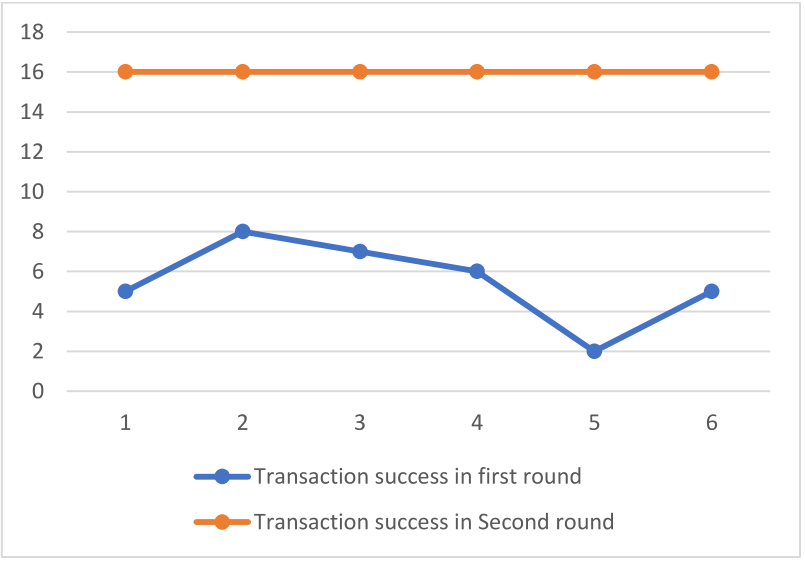

Fig. 5. Experimental Results of the Shamir Threshold Scheme Verification System Security Performance.

- The five intermediaries are being used as detecting keys to determine whether the user's secret is valid. The remaining 80 valid subkeys and 20 incorrect subkeys are distributed to 100 users. The person's sub-key is exchanged by creating a random integer to provide the outcome of a random process of the sub-key. The 80 users who received the proper subkey are trustworthy, but the 20 individuals who received the incorrect subkey are corrupt and will manipulate others from the deal.
- Here, for instance, predict a significance difference on Privacy-Protected Blockchain Systems among these 100 people. A set of five individuals uploads their own key and begins the first round of trade. If the team is successful in reconstructing K, it signifies that the team is able to accurately modify the data of the cryptographic protocol activity and confirm that all involved users are truthful users after decoding. If the team is unable to effectively rebuild K, it demonstrates that the team's users are deceivers, but every user with in group can be examined immediately.
- Identify all of the scammers' IDs and eliminate all deceivers again from user.
- Distribute the other users at chance, five each group, but then begin the next round with trade.

Experiment results show from Fig. 5 that if the Privacy-Protected Bitcoin System is not utilized to eliminate deceivers, the success chance of each round of trade is low with only two transactions in the lowest round being effective, as well as the rate of success as low as 10%. Using a Privacy-Protected Blockchain Network, the deceivers may be correctly removed from the users. Just after deceiver has indeed been eliminated, each unit can effectively recreate K with a transaction's success frequency of up to 100% in the next round and operations.

The Privacy-Protected Blockchain Network eliminates the deceiver and ensures that each following transaction is sturdy and healthy. The Privacy-Protected Blockchain Network may perform its role extremely well in the replicated transactions employing the secret key of the Shamir threshold scheme as the transaction object, that is, protecting the user's privacy information and completing the execution of the deceiver.

1. Decision-Making and Trust in blockchains

Bitcoin, and blockchains in particular, assume that all networks are equally untrustworthy and that their share of the collective decision-making process is purely determined by their computational capacity (known as the Proof-of-work algorithm). In other words, for each node r, $trust_r \propto$resources(r) (based on probabilities) determine the node's support weight. This has negative consequences, including vulnerability to sybil attack, exorbitant energy usage, and network latency.

Proof-of-Work assumes that networks who invest considerable resources in the network become less likely to steal. Using similar logic, we may devise a new variable measurement of confidence, based on link behavior, in which good actors who adhere to the protocol are rewarded. In particular, each node's trust might be set as the predicted value of it performing properly in the future. As we're working with a binary stochastic process here, the anticipated value becoems just the probability p. Counting the amount of good and negative actions taken by a node and using the sigmoid activation function to compress it into a probability is a simple technique to estimate this probability as shown in Eqn (1).

$$trust_r^{(a)} = \frac{1}{1 + e^{-\alpha(\#good - \#bad)}}, \tag{1}$$

Where α is simply the step size.

With this approach, the system might assign trusted nodes more weight and calculate blocks more quickly. As building confidence

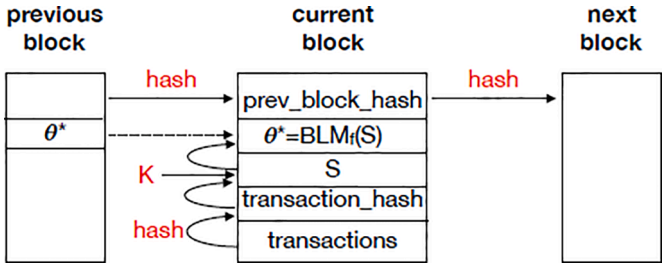

Fig. 6. PoW Block [25].

in a system takes time, this should be immune against sybil attacks. This technique may invite other sorts of attacks, including such nodes building their popularity in order to act maliciously afterwards. This could be avoided by randomly choosing many nodes to participate on each transaction, graded by their confidence, and then accepted the equitably democratic majority. This should keep single actors from wielding too much power, irrespective of the level of trust.

This section discusses about the future recommendations to develop highly matured distributed system using blockchain.A major contribution in the proposed system is the way of overcoming the blockchain's public nature. The proposed system can be suitable for storing and random querying, but it does not suit for data processing. It is important to know that when a service queries the data, it would be stored for future analysis. For privacy preservation, a service should not be allowed to learn about the raw data. However, it can be allowed to directly compute within the network to get the final result. If the data has been split into shares, then a secure Multi Party Computation can be used to evaluate the data safely.

It is assumed that in blockchain each and every node is untrusted equally and the proportion in the process of decision making depends only on the computational resources. This is called as the Proof-of-Work (PoW) as shown in Fig. 6. This causes sybil attack, high latency and high consumption of energy.The PoW represents that the node supplying substantial resources have fewer chances to cheat.Like this, a dynamic trust measuring system has been implemented, based on the behavior of nodes. It means the nodes that correctly follow the protocol will be rewarded. Also, in future, the trust of each of the nodes is to be established which isthe probability of the nodes to perform well. This probability value can be calculated by the count of total good and bad actions performed by the nodes by using a sigmoid function. By this way, a network can get more weight to trusted nodes and can facilitate efficient block computation. As the time taken to get the trust is more, this system highly resists the sybil attacks.

$$D = \{D_1, \ldots,\ D_k, D_1, \ldots, D_k \epsilon \{1, 2, \ldots, N\} \tag{2}$$

D is the set of dimensional indices as shown in Eqn (2) which defined the Subspace with K-dimension,θ*εθ is a bounded local minimum (BLM), if

$$x(\theta^*) < x(\theta) \tag{3}$$

Where,

$\theta = (\theta_1, \theta_2, \ldots, \theta_N)$, and *f denotes*the objective function as shown in Eqn (3)

Nevertheless, this method might attract other attacks, like the nodes that increase their reputation so as to be malicious later. It can be moderated by a majority voting system, in which the nodes are selected randomly and weighted by their trust for voting [25]. Finally, vote with equal weight will be selected,it will thereby avoid a single node getting more inspiration irrespective of their trust.

6. Conclusion

In general, third parties should not be trusted in terms of personal and sensitive data storage. Such data stored or shared via trusted third parties are susceptible to security attacks. Here, the users should be the owner of their data. In this case, there should not be any compromise in security and should not be any limitations in providing personalized services by the authorities.The proposed Blockchain Based Decentralized Personal Data Management System works as an access-control moderator combined with an off-blockchain storage system. None of the users are needed to trust any kind of third parties. Also, as the owner of the data, they will be anytime aware of the data gathered from them and its usage. Hence, the organizations can focus only on how the data is to be used instead of focusing on how it is to be secured or categorized. The major advantage of using decentralized system is that formulating regulatory and legal decisions to collect, store and share the personal data are highly simpler here.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review 2008:21260.
[2] Böhme R, Christin N, Edelman B, Moore T. Bitcoin: economics, technology, and governance. J Econ Perspect 2015;29(2):213–38.
[3] Ali ST. Bitcoin: perils of an Unregulated Global P2P Currency (Transcript of Discussion). In: Cambridge International Workshop on Security Protocols; 2015. p. 294–306.
[4] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. Ieee Access 2016;4:2292–303.
[5] Kaaniche N, Laurent M. A blockchain-based data usage auditing architecture with enhanced privacy and availability. In: 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA; 2017. p. 1–5.
[6] Yasin A, Liu L. An online identity and smart contract management system. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). 2; 2016. p. 192–8.
[7] K. Kuikkaniemi, A. Poikola, and H. Honko, "Mydata a nordic model for human-centered personal data management and processing," 2015.
[8] Mamoshina P, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 2018;9(5):5665.
[9] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: using blockchain for medical data access and permission management. In: 2016 2nd international conference on open and big data (OBD); 2016. p. 25–30.
[10] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 2016;40 (10):1–8.
[11] Zhu L, Wu Y, Gai K, Choo K-KR. Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems 2019;91:527–35.
[12] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: decentralized computation platform with guaranteed privacy," *arXiv preprint arXiv:1506.03471*, 2015.
[13] B. Faber, G.C. Michelet, N. Weidmann, R.R. Mukkamala, and R. Vatrapu, "BPDIMS: a blockchain-based personal data and identity management system," 2019.
[14] Truong NB, Sun K, Guo Y. Blockchain-based personal data management: from fiction to solution. In: 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA); 2019. p. 1–8.
[15] Onik MMH, Kim C-S, Lee N-Y, Yang J. Privacy-aware blockchain for personal data sharing and tracking. Open Computer Science 2019;9(1):80–91.
[16] M.H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *arXiv preprint arXiv:1801.03528*, 2018.
[17] Miraz MH, Donald DC. Application of blockchain in booking and registration systems of securities exchanges. In: 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE); 2018. p. 35–40.
[18] Onik MMH, Miraz MH, Kim C-S. A recruitment and human resource management technique using blockchain technology for industry 4.0. In: Smart Cities Symposium 2018; 2018. p. 1–6.
[19] Joshi KP, Gupta A, Mittal S, Pearce C, Joshi A, Finin T. Semantic approach to automating management of big data privacy policies. In: 2016 IEEE International Conference on Big Data (Big Data); 2016. p. 482–91.
[20] Benhamouda F, Halevi S, Halevi T. Supporting private data on hyperledger fabric with secure multiparty computation. IBM J Res Dev 2019;63(2/3). pp. 3–1.
[21] Zyskind G, Nathan O, "Sandy" Pentland A. Decentralizing Privacy: using Blockchain to Protect Personal Data. In: 2015 IEEE Security and Privacy Workshops; May 2015. p. 180–4. https://doi.org/10.1109/SPW.2015.27.
[22] Gilani K, Bertin E, Hatin J, Crespi N. A survey on blockchain-based identity management and decentralized privacy for personal data. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS); 2020. p. 97–101.
[23] E. Karaarslan and E. Konacakli, "DATA STORAGE IN THE DECENTRALIZED WORLD: BLOCKCHAIN AND DERIVATIVES," p. 33.
[24] Salman O, Elhajj I, Kayssi A, Chehab A. An architecture for the Internet of Things with decentralized data and centralized control. In: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA); 2015. p. 1–8.
[25] Wei Li, Adapting Blockchain Technology for Scientific Computing, arXiv:1804.08230, pp 1–8.

Anna Gustina Zainal currently serving as a Lecturer at the Department of Communication Studies, University of Lampung, Indonesia. Various scientific works have been published in reputable national and international journals.

Ricardo Fernando Cosio Borda holds Doctor of Management. Management Professional School Director of the Universidad Autónoma del Perú. Project Management Master's student. Operations Manager of Laboratorios Sostenibles para América Latina. Certified Green Project Manager, GPM-bTM. Visiting professor at the Universidad Nacional Autónoma de México (UNAM). Author of scientific articles published in indexed journals.

Yousef Methkal Abd Algani finished his Ph.D. in Mathematics education. He completes his Teaching Certificate, and in addition to a Certificate on Measurement and Evaluation in Education in Oranim Collage. He participated in several international conferences, and he published many articles in the field of Applied Mathematics and Mathematics Education

Bhaskarrao Yakkala is currently working as an Assistant professor at Saveetha School of Engineering, Chennai. He is a passionate teacher and has over 10 years of teaching experience and 2 years as a research analyst. He has over 30 Publications in various Scopus – indexed journals and in a web of science. He actively participated in many international and national conferences, workshops, and webinars.

Sanjith S, holding a doctoral degree in Computer science and Engineering, currently working as an Assistant Professor & Head Department of Computer Science in St. Alphonsa College of Arts and Science, Karinkal. Independent Researcher having memberships in Scientific Societies, published various research articles both in national & international levels. Research interest are Image Processing, Wireless Sensors and Networking.

Iskandar muda the chief researcher, Professor of Accounting at the University of Sumatra Utara. His-qualification is Secretary of the Master of Accounting Studies Program and Secretary of the Doctor of Accounting Science Program, University of Sumatera Utara.

T. Kalaichelvi awarded Doctor of Philosophy (Ph.D.) in Computer Science and Engineering by Sathyabama University, Chennai, India in the year 2014. She is currently working as Professor Grade in Head of Department of Artificial Intelligence and Data Science at Panimalar Institute of Technology, Chennai, India. Her areas of interest include Data mining, image processing, IoT, Deep Learning, Data Analysis, and cyber security.

B. Kiran Bala, presently working as a Head of the Department, Department of Artificial Intelligence and Data Science, K.Ramakrishnan College of Engineering (Autonomous), Trichy, Tamil Nadu, India. He has having 10 years of Teaching & Research Experience and also published more than 50 papers in peer reviewed journal. He attended so many International Conferences, Workshop etc.