International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A BLOCKCHAIN-BASED SECURITY SHARING SCHEME FOR PERSONAL DATA WITH FINE-GRAINED ACCESS CONTROL

C. Rashmi1, K. Sai Vineela2, D.Keerthi3, M Hema Haritha4

1Assistant Professor Department of Information Technology Malla Reddy Engineering College for Women (UGC-Autonomous) Maisammaguda,Hyderabad, TS, India.

2,3,4 UG students Department of Information Technology Malla Reddy Engineering College for Women (UGC-Autonomous) Maisammaguda,Hyderabad, TS, India.

ABSTRACT: Only a few keywords may currently be used to search blockchain-based encryption. Thanks to distributed storage on the blockchain, users can disseminate the data without a centralized server. Both the cloud server and the user have mutual mistrust in one another because they are concerned about losing control over the personal data that has been outsourced. Secret service providers were unable to evaluate personal information under the current circumstances. One of the most frequent problems was trying to find encrypted cloud services. Contrarily, because the traditional cloud storage approach uses centralised storage, a single point of failure might bring the entire system to a standstill. The emergence of blockchain technology has actually led to a greater level of public awareness of decentralised storage. Decentralized storage has several advantages over central storage, including low cost and quick throughput, and it can address the issue of a single point of failure in traditional cloud storage systems. The only person who can download the material and decode it is someone whose features comply with the accessibility policy. The data owner has fine-grained access control over his or her information, and the BSSPD offers an attribute-level retraction of a specific data individual without affecting others. The ciphertext key words search is performed while obtaining data to further protect the privacy of the data subject. We verified the security of the BBSPD and assessed our strategy on the EOS blockchain, which demonstrated its viability. We also performed a thorough analysis of the processing costs and storage costs, which demonstrated the effectiveness of BSSPD.

Keywords: Block chain, BSSPD, encryption, cloud service, ciphertext, high security.

I INTRODUCTION:

The development of 5G and Internet of Points contemporary technology offers a significant amount of training data for the speedy development of artificial intelligence (AI). Data security and privacy protection have become one of the most fascinating topics of discussion in data sharing and management. Solid data mining and analysis have really exposed potential threats to the protection of individual privacy. Most clients typically choose to outsource their data to cloud web servers for sharing and circulation. However, the majority of data stored in the cloud is extremely sensitive, particularly data produced

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

by IoT devices that are tightly connected to human life. These details are special and may include private information about a person's life, job, and health and well being; if private information is seized or unlawfully disclosed and connected to the real identity of the data owner, it can result in a great deal of issues for a person. As a result, all contemporary businesses using big data and AI today face enormous challenges integrating data, creating value, and maintaining data security and privacy.

Academics have recently presented a number of safe and secure sharing solutions in the context of the cloud. [1-- 9] These techniques seem to address the concerns regarding safety and privacy when sharing information. However, they all have the same flaw: they are too reliant on the Cloud Service Provider (CSP). They believe the CSP to be a trustworthy third party and base their security models on the assumption that the CSP is only partially trustworthy, meaning that it will be interested in the data but won't delete it. It shows that there is always a chance that the current circumstances will change.

(1) The CSP may personally profit financially from the user's personal information, or its employees may violate customer privacy rights. Despite the fact that some techniques, such attribute-based security algorithms, appear to be user-centric and offer user-defined access limits, these techniques still require a dependable third party to generate and manage user keys. It is possible that these trustworthy facilities will work together in the future. Once the data is transferred to the cloud web server, each of these will unavoidably result in the data owners losing complete control of their information.

(2) The CSP manages the data on cloud servers and centrally stores it. Inevitably, a single point of failure could prevent users from regularly using cloud services to access their data. Disaster recovery backup can help the CSP improve service security and data protection. However, some inescapable factors, like political ones, will deter customers from using cloud solutions to access their data.

(3) The CSP must spend more money on web servers, better personnel, the upkeep of information centre infrastructure, and other things in order to offer better service. These costs are escalating along with the CSP expense and the creation of the management platform. Customers eventually pay for the CSP's operational costs.

OBJECTIVE OF THE PAPER:

Each blockchain, distributed network, and cloud computing has distinct characteristics and faces similar network-related challenges. [4] A further level of protection that incorporates numerous network-related technologies may be provided by future assimilation. Despite the possibilities of diverse adversarial tactics, some cyber hazards in cloud computing, such as identity theft and information mining-based assaults, also place on blockchain networks. [5] The data stored in blocks and made available to authorized users hints that mining block data can violate users' privacy. The situation is the same when data is stored on faraway cloud web servers. A successful connection attack on a private cloud dataset could result in privacy

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

leaking. [6] Consequently, two current technologies are in danger due to both internal and external issues. Cloud computing resources are added to the blockchain system to improve security, performance, and solution level. Hardware in computer systems refers to any device connected to a block chain and is just as important as software. [7]

II RELATED WORK

[1] Zhipeng Cai, Zaobo He, Xin Guan, and Yingshu Li act as the judges for collective data sanitization for social media attacks that aim to suppose delicate details.

The leak of user data from social media networks could seriously violate their privacy. User profiles and friendships are both by their very nature private. Sadly, sensitive information from publicly accessible data can be predicted by data mining technologies. As a result, network data needs to be cleaned up before being published. In this article, we examine how to unleash a logical assault using social networks that combine non-sensitive features and social communications. We relate this challenge to a problem of group categorization and offer a model of group reasoning. Using user accounts and their social connections, an attacker can predict sensitive information about connected victims in a publicly available social media network dataset, according to our method.

Zhipeng Cai, Xu Zheng, and an additional participant from the student audience continue to be present as they discuss [2] a secure and reliable method for posting information in intelligent cyber-physical systems.

Information submission in intelligent cyber-physical systems faces new difficulties in terms of energy conservation and privacy protection in order to enable granular access to various areas of the physical environment. People must send information using the least amount of power possible. However, focusing solely on energy efficiency could result in the extreme disclosure of personal information, especially given that participant-uploaded content is currently more revealing than ever. In this article, we propose a novel information dissemination strategy for intelligent cyber-physical systems that takes into account both power efficiency and privacy protection.

[3] In order for taxi companies to approximation metropolitan website traffic streams, a differential-private structure is required. Jiguo Yu3,4,5, Zhipeng Cai3, Xu Zheng2, and Athors Participant

As a result of the enormous expansion of public transportation systems, cab traffic may now serve as a credible indicator of urban population trends. The general public, city officials, and the actual taxi businesses will all find this information to be of great use. However, the confidential information of taxi firms is seriously at risk if such web content is disseminated carelessly. They will undoubtedly divulge both their own market ratios and the private information of both traveller and drivers. Therefore, in this study, we propose a novel framework for taxi services to share traffic while

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

safeguarding privacy, which takes users' privacy, profits, and justness into account.

CURRENT SYSTEM:

There is now a structure in place for the storage and exchange of EMR data for cancer patient care. It uses cloud services to store the encrypted data and a permission chain to maintain metadata and accessibility control rules. People can specify their accessibility control policies to ensure information security and accessibility. The block chain-based data-sharing schemes discussed above provide a great framework, but most of them only outline the strategy without describing how the necessary protocol will actually be put into practise.

SYSTEM RECOMMENDED:

Open commerce and information security confirmation are essential in an AI-powered environment. Customers transfer their data to a cloud web server for limiting and also distributing, which necessitates the use of a standard data sharing organization stage. Clients would lose control of the information once it left the server, raising major safety and security as well as insurance policy issues. Access control and data security are regarded as sophisticated improvements for storing specific information on cloud internet servers, but their use is limited. But for the most part, it still depends on the Cloud Provider, namely a Fourth Party (CSP). To address this issue, they used the Interplanetary Files System, 3DES ciphertext technology, blockchain, and ECC (IPFS). Details of the BTDEC Trible This study focuses on the Elliptic Contour Crypto-system for Personal Data. This customer-driven strategy enhances the decentralization of the system by requiring the information bearer to wait on IPFS while safeguarding the sharing data. According to the built-in confirmation mechanism, the shared data area and decryption key will be connected using 3DES and also ECC, and the information owner will distribute his data-related information and transfer on ways to information users using blockchain. The only information client allowed to download, instal, and evaluate the information is one whose credit score scores fulfil the verification norms. By enabling the information owner to refuse a specific information customer at a precise measurement without affecting other customers, BTDEC grants the owner of the information fine-grained network access control over his information. They verified the validity of the concept by examining BTDEC's security and replicating our current technology on the EOS blockchain. To preserve the privacy of the information customer, the ciphertext phrase search is frequently used when obtaining information. They looked at the costs and constraints at this time and discovered that BTDEC performed admirably.

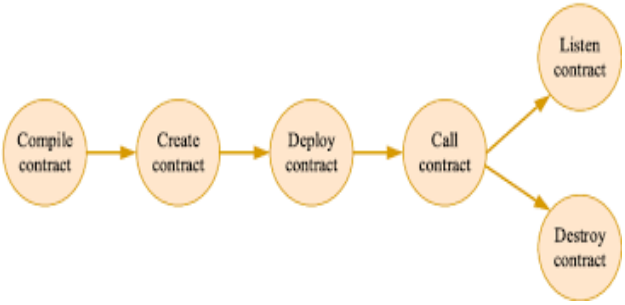


Fig.1. Block chain model.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

III METHODOLOGY

They have actually created the following technique: The IPFS, blockchain, information owner, and data customer are the four components of BTDEC. The DO quickly shared his information to IPFS, saved it using a blockchain smart agreement, and unlocked the key using a decryption tool. A fine-grained availability to details control is implemented using 3DES and ECC. Only those who meet the admittance requirements can acquire and also decrypt the traded information because it has been compressed to the DO's blockchain. The process is distributed across. To provide information security and transparency, the data is supported by and saved in the IPFS. The unchangeable DO and DU are stored on the blockchain.

The following tasks are explicitly managed and carried out by these 4 locations: Create a safe and secure hoarding solution with IPFS. The driving force's organization structure ensures that IPFS proficiency can never be restricted.

Blockchain: The blockchain manages all newly added information to the plan as well as any information that is currently accessible to the broader public. It's possible that similar methods were initially used to deliver safe and secure messages from DO to DU. This is the main tactic, even though there could not be a single genuine outsider to be found. In BTDEC, there are essentially 2 types of smart contracts. DSContract receives customer information from UMContract, which keeps track of them.

Owner of the data: according to the approach, this individual is in charge of directing the creation and distribution of the Smart Arrangement. The DO's institutional capabilities and the systems he has in place for disseminating information with those who have access to it are both open to question. A data person (DU) can also ask for entrance permissions, which the DO might grant or deny, in order to use common data. The location and also approach to obtaining the common knowledge will be made known when DU's characteristics link the strategy indicated in the ciphertext. The entire client ID was only provided as part of the 3DES, ECC mechanism to handle authorization denial. The countersign ciphertext search provided by BTDEC helped it operate.

The following overview discusses each novel element:

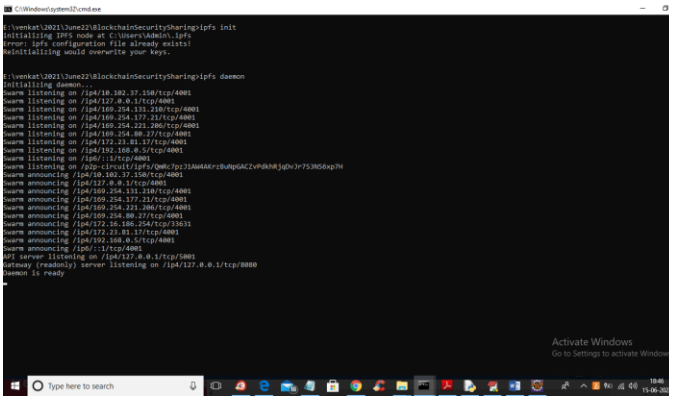
1 The Division of the Interior is in charge of creating as well as disseminating innovative agreements. Each person in our setup has two Smart Agreements. Because of the value of the administrators, the inventiveness of the board, and the involvement of the users, UMContract is well-liked. DSContract keeps an eye on all information transmission, access plan changes, authorization denials, and information retrieval operations.

After the DO generates the setup personal keys and also residential properties public key on the area, the structure public trick is saved in DSContract.

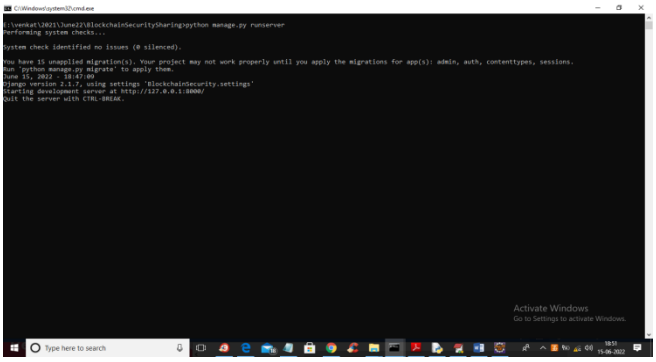
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

IV IMPLEMENTATION

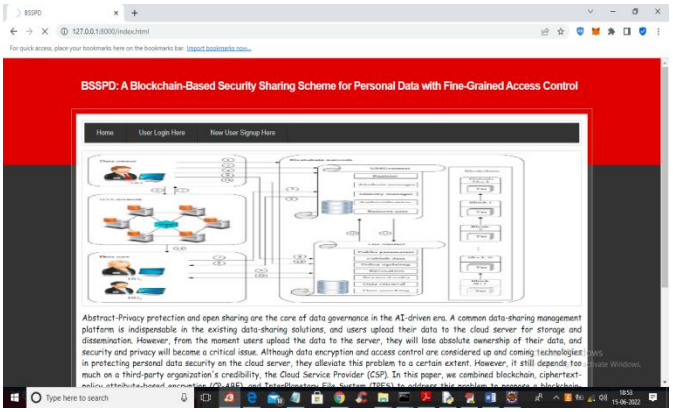
To launch the project, double-click the "Start IPFS.bat" file to launch the IPFS server and display the screen below.



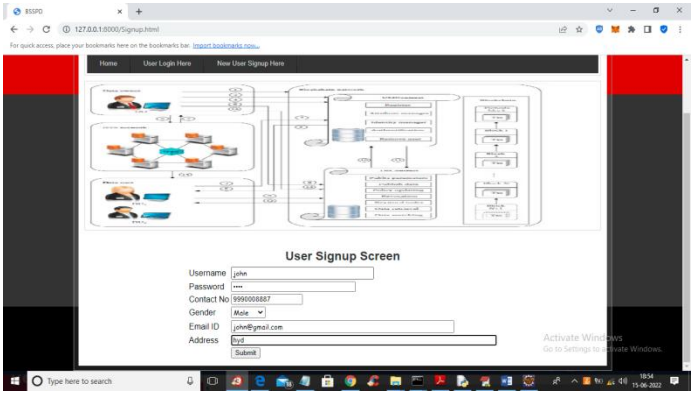
The IPFS server is now running on the screen above. Next, start the Python DJANGO server by double clicking the "runServer.bat" file.



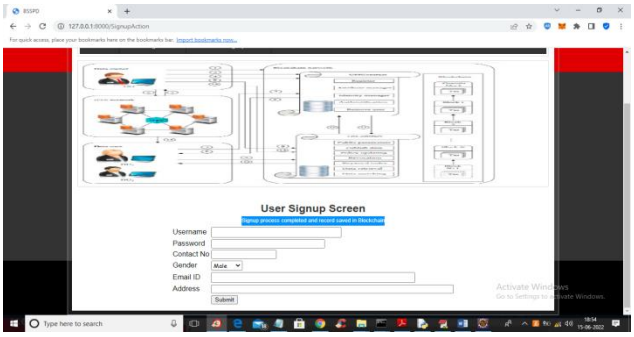
Python DJANGO server is now running in the screen above. To access the screen below, open a browser and type the URL "http://127.0.0.1:8000/index.html" into the address bar.



In above screen click on 'New User Signup Here' link to add new user to Blockchain

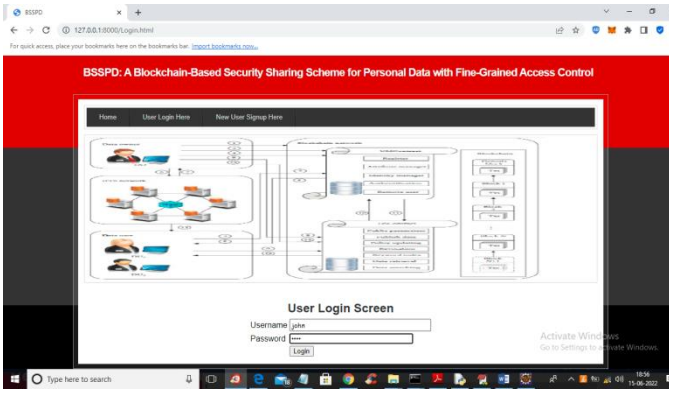


In above screen user is signup and press button to get below output

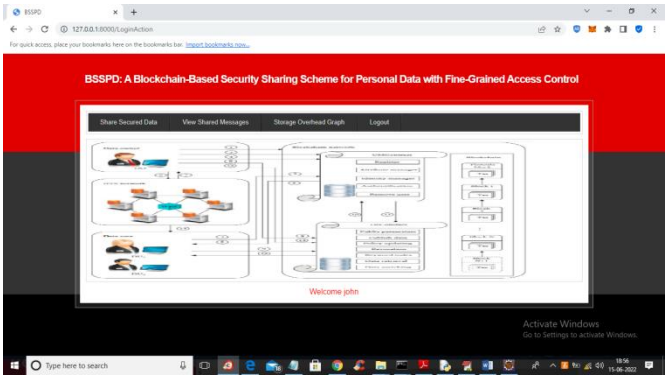


In above screen user signup process completed and similarly you can add any number of users and now click on 'User Login Here' link to get below login screen

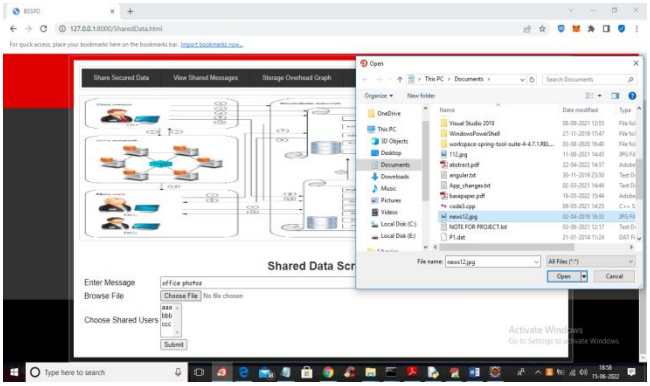
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



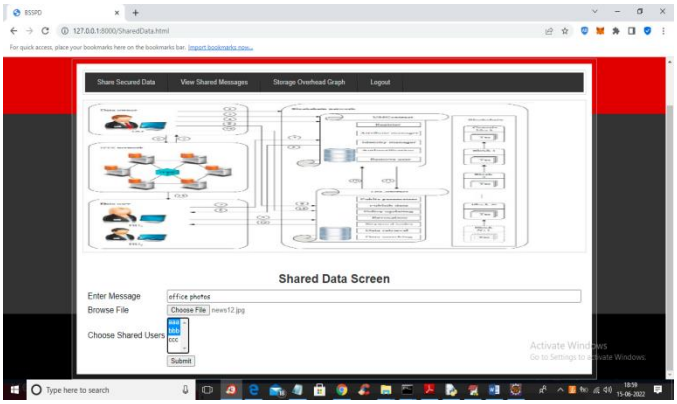
In above screen user is login and press button to get below output



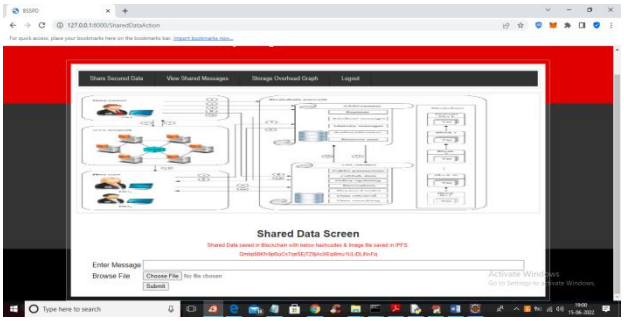
In above screen user logged in successfully and now click on 'Share Secured Data' link to share data with other users



The user can type text and upload images on the aforementioned panel, and by holding down the CTRL key while doing so, they can choose which users they want to share the data with. Pressing the button will result in the results seen below.



In above screen 'John' is sharing data with user 'aaa' and 'bbb' and both users can decrypt and view data but user 'ccc' cannot view it.



The sharing qualities are saved on the Blockchain, while the IPFS stores the photos and decryption keys. Click the "View Shared Messages" link to view your own and other users' shared messages. Since "John" is the data owner, he can see both his own upload and other users' shared data.

V CONCLUSION

In the AI-driven future, a stakeholder-sharing perspective is presented to promote comprehension while ensuring data security. By

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

merging the blockchain, BTDEC, and IPFS, I proposed a block chain-based security sharing information system for reasonably effective authorization management as well as additionally approval cancellation. The DO uses the approved approach to submit his information to IPFS while keeping it secure. He then encrypts the technique and uses 3DEECS to decode the return address. DUs that meet the requirements of the admission procedure are required to gather information and encrypt it. The method has no embedded control centre, and the DO has complete discretion over the information he shares, safeguarding both security and personal privacy. To illustrate this point, they created this framework on the EOS blockchain. Defense and execution evaluations show this strategy's reason ability, vigour, and dependability. It might also make use of virtual currency to increase the scope of this approach and create a system of trade for information. Besides that, there are a few issues with this strategy. For instance, the 3DEECS, which were created with revocable authorization, are insufficient. On BTDEC, numerous research assignments have been completed. For this method, a 3DEECS with an additional obvious execution would be beneficial. 'the's' is an a. For each and every information transmission, it would also be necessary to manage a huge number of datasets, but this effort might be accomplished more quickly. Blockchain has been suggested as a solution to the reasonableness issue with the present document encryption technology by a number of researchers.

VI REFERANCES

[1] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," in Computers & Security, 2018, vol. 72, pp. 1–12.

[2] S. Sundareswaran, A. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," in IEEE Transactions on Dependable and Secure Computing, 2012, vol. 9, no. 4, pp. 556–568.

[3] Cheng-Kang Chu, S. S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," in IEEE Transactions on Parallel and Distributed Systems, 2014, vol. 25, no. 2, pp. 468–477.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1–9.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," in IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.

[6] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," in IEEE Transactions on Dependable and Secure Computing, 2018, vol. 15, no. 4, pp. 1–590.

[7] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," in IEEE Transactions on Network Science and Engineering, 2020, vol. 7, no. 2, pp. 766–775.

[8] X. Zhou, W. Liang, K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big

data," in IEEE Transactions on Emerging Topics in Computing, no. 1, 2018.
[9] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flow estimation via taxi companies," in IEEE Transactions on Industrial Informatics, 2019, vol. 15, no. 12, pp. 6492–6499.
[10] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf.
[11] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchainenabled de-duplicatable data auditing mechanism for network storage services," in IEEE Transactions on Emerging Topics in Computing, 2020.
[12] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," in IEEE Transactions on Services Computing, 2020, vol. 13, no. 2, pp. 289–300.
[13] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," in IEEE Transactions on Network Science and Engineering, 2020.
[14] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," in IEEE Transactions on Industrial Informatics, 2019, vol. 15, no. 6, pp. 3632–3641.
[15] M. Swan, "Blockchain thinking: the brain as a decentralized autonomous corporation [commentary]," in IEEE Technology and Society Magazine, 2015, vol. 34, no. 4, pp. 41–52.