Annals of Library and Information Studies
Vol. 67, December 2020, pp. 257-267

Securing Online Knowledge Systems by Blockchain: a proposed solution for model Online Defence Information System

Gopal Bhushan[a] and Margam Madhusudhan[b]

[a]Outstanding Scientist & Director, DRDO-MED and Computational Systems, New Delhi - 110054, Email: g.bhushan@odisys.in

[b]Associate Professor, Department of Library and Information Science, University of Delhi, Delhi - 110007, India

Received: 27 August 2020; revised: 13 December 2020; accepted: 19 December 2020

Information systems offer a range of services by amalgamating information, technology, people, and organizations to serve business needs to solve problems, and disseminate knowledge within and in public. Certain unclassified but restricted information could also be made available on these systems/platforms to a class of pre-authenticated registered users. The model Online Defence Information System (ODIS) (https://www.odisys.in) is one such system that is the basis of discussion in the paper. It is designed and developed as an important knowledge resource for defence community. An expert can also contribute by making online submissions of tacit knowledge for the benefit of society. The system is built on the centralized networking architecture and is based on trust management (trust of content and platform). Given the security vulnerabilities rising proportionally with computational power, it has been established that a centralized system is more likely to see malicious attacks than a decentralized system. Paper explores the solution to counter apparent vulnerabilities and draws an analytic comparison with "blockchain", decentralized network architecture. The paper gives an overview of ODIS's architecture, development and design methodologies and challenges, and a solution that offers safety, security, authenticity and verifiability of contents on the system such as ODIS.

Keywords: ODIS; Defence community; Information systems; Open access; Knowledge management; Blockchain; Digital asset; Client-Server; Peer-to-Peer

Introduction

The evolution of communication and resultant decision making has transcended many eras of computer communication, from pre-internet to "peer-to-peer"[1]to recent phenomena called blockchain. The pre-internet era was the era of human to human, fixed telephony, and face to face communication, albeit considerable time consuming and delayed decision making. The internet introduced the World Wide Web, TCP/IP Protocol[2], email, client-server[3] architecture, and a single point of failure but trust deficit. The peer-to-peer age brought distributed application architecture[4] and the sharing of networks that saw challenges due to network vulnerability and remote accessibility.

Blockchain is a decentralization network methodology that has revolutionized communication by transferring assets, i.e., it records transactions and tracks assets digitally. The difference between a distributed and decentralization network is that the former is a technical arrangement of laying the nodes. At the same time, the latter is a concept that is built upon the former. A knowledge management system that delivers online content has to ensure the origin and integrity of data/content. An online post, if compromised, it is conjectural to assume that data it provides has doubtful integrity and it becomes important to establish the origin of the data and with an established IAM (identity access management). The paper discusses blockchain-based ODIS, where information authenticity and veracity would be ensured. The succeeding paragraphs explore technologies those would ensure that data provided on ODIS, an open public platform, was authentic and meets the expectation of users of authentic information for that might be used for scholarly work and decision-making process.

Review of literature

The integration of classical security measures with the blockchain technology, provides a unique secure solution. This study compares one another to set the narrative and later, cross analyses the blending of two. The narrative leads to challenges apropos for the ODIS and similar online systems.

A knowledge management system that delivers online content has to ensure the origin and integrity of data and content. Data integrity and data confidentiality is central to any online system for being regarded a trusted platform. The centralized knowledge management systems have severe security and privacy concerns.

Elisa et al.[5]writes, online systems or websites which are based on centralized architecture, suffer from a single point of failure and make the system a target to cyberattacks such as malware, denial of service attacks (DoS), and distributed denial of service attacks (DDoS).These systems needed to be distributed, secured and privacy-preserved and that is achievable with decentralization, peer-to-peer (p2p) resource sharing using the blockchain technology, for assurance of both information security and privacy and a trustworthy platform. The blockchain technology enables the implementation of highly secure and privacy-preserving decentralized systems where transactions are not under the control of any third-party organizations. Using the blockchain technology, existing data and new data are stored in a sealed compartment of blocks (i.e., ledger) distributed across the network in a verifiable and immutable way. Information security and privacy are enhanced by the blockchain technology in which data are encrypted and distributed across the entire network. (Elisa et al.[5]).

Miles[6]describes, a blockchain, is a chain of digital "blocks" that contain records of transactions and each block is connected to all the blocks before and after it. This makes the chain rather robust and tamper proof. Besides, the records on a blockchain are secured through cryptography and participating nodes have their own private keys, and, if a record is altered, the signature will become invalid. Importantly, blockchains are decentralized and distributed across peer-to-peer networks that are continually updated and remained in sync and therefore, don't have a single point of failure. However, it remained to be seen that the infrastructure on which the blockchain framework rests is equally robust and secured and does not have vulnerabilities which can be manipulated for devious design [6].

Lage et al.[7] have analyzed various facets of blockchain and how blockchain can be useful to achieve security requirements typically, in the realm of backup and recovery, threat intelligence and content delivery networks. The paper talks about the advantages accrue with the use of blockchain and how adopting a network with such all complexity remains a preferred choice where failure cannot be afforded for its devastating effects economically and services it provides. Fundamentally, it could be safe to assume that a decentralized blockchain based system is impregnable because of the network is composed of multiple participants that reach a common consensus without the intervention of a central authority, however blockchain is not a pinnacle. It may not be the right solution for systems governed by a single central authority or to store data whose integrity and source is not relevant[7].

To address such issues, a centralized cyber security protection scheme can be adopted or similar security measures can be implemented at different cloud layers in case of cloud-based architecture. Other alternatives are DLT (Distributed Ledger Transaction) models; most important among them is blockchain. Blockchain uses bitcoin technology to build scalable, decentralized applications. The blockchain was introduced by Satoshi Nakamoto[8] in 2008 for using cryptography applications to provide security, confidentiality, end-to-end encryption and real-time alert for security breaches.

The sectors, where blockchain is already in use are finance[9], banking, payment-transfers, bitcoin technology and entertainment industry such as online music streaming, IoT; and social sectors like health care[10], real estate, education[11], law enforcement, digital IDs, etc. The emerging fields are supply chain[12], audit trail, copyright and royalty, taxation and equity trading[13] and S&T[14]. Blockchain was improved in its design to include timestamp blocks without requiring them to be signed by a trusted party. It also introduced a difficulty parameter to stabilize the rate with which blocks are added to the chain[15]. The time stamp ensures that data/documents/information transmitted was not tampered with. The following year, the design was implemented as a core component of the crypto currency bitcoin, where it serves as the public ledger for all transactions on the network[16].

The words "block" and "chain" were used separately in Satoshi Nakamoto's original paper, but by 2016, it was eventually popularized as a single word, blockchain. Blockchain has also shown that digital assets (digital representation of any data) can be handled and transferred even on an open network (sans security layers). Bitcoin core and Ethereum

public blockchains[17] and widespread adoption of Corda and Hyperledger blockchain[18] by companies like IBM offer data authentication and provenance are considered important aspects for defence applications offered in the public domain.

Objectives of the study

While transacting, both information and/or data are susceptible to manipulation. Overarching security architecture of blockchain, aims to provide encompassing protection of identity, data, and infrastructure. The study aims to cover the following broad objectives and suggest implementation of blockchain for underlying security and protection.

- To study problems of online centralized knowledge management systems;
- To explore alternatives for effective cyber security in the context of knowledge management systems;
- To explore mechanisms for assuring safety and security of the tacit knowledge shared on centralized knowledge management system;
- To investigate methodologies for authenticity, provenance of the content hosted on centralized knowledge management systems and the contributors' privacy;
- To study provisions to counter the challenges of knowledge storage and sharing in public domain; and
- To provide a solution that offers safety, security, authenticity and verifiability of contents on the centralized knowledge management system.

Comparison of architectures: client-server & peer-to-peer

ODIS, in its present form, is based on client-server architecture, which serves clients' requests (the nodes on the network) from the server (the central server on the network). The proposed blockchain arrangement is a decentralized system based on “peer-to-peer architecture where nodes are peers of each other and no node has supremacy over others”[19].Fig.1 depicts typical architectures of two arrangements.

Data integrity and data confidentiality is central to any online system for regarded a trusted platform. Blockchain provides a strong case in all areas (performance, security, data integrity, privacy, authentication, and provenance, etc.), which concerns a developer and the client.

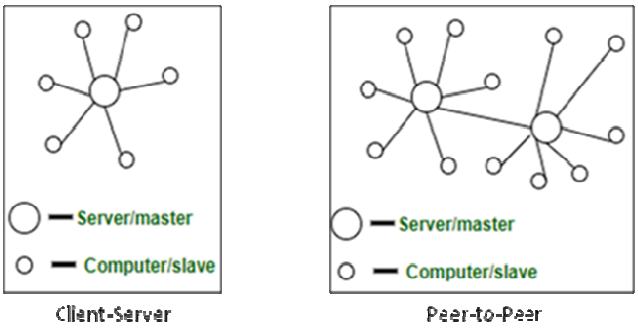

Fig.1 — Client-server & peer-to-peer architecture (Source: https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems) (Accessed on 15/5/2020)[19]

The present study has analyzed various aspects of centralized and decentralized systems (blockchain), making the basis for using blockchain to improve the existing ODIS.

The design and development of a model ODIS

The model ODIS has been designed and developed as a single point repository on defence for the defence community which largely embodies a vast pool of professionals representing defence scientists, researchers, and engineers, personnel from civil defence, armed forces, strategic thinkers, academicians, scholars, corporate managers, and from other sectors like industry, commerce and foreign affairs. The subjects/topics which have been catered to are, (i) defence sciences, research and engineering, (ii) defence products, technologies and innovation; (iii) domestic & international legislations on defence export; (iv) international defence R&D cooperation and defence industry, (v) disarmaments and arms control; (vi) international defence/ military academia and strategic perspective on global peace and security etc.

The need-assessment survey helped in understanding the interests and concerns of users. ODIS has drawn on the experiences of defence professionals on qualitative and reliability aspects of existing online systems and has taken into account the extent of their usability and feasibility in developing a better system with improved functionalities to translate expectations and experiences into ODIS’s architecture. The assessment and integration of ideas and their coherency were evaluated for fuller definition towards developing a robust platform. The underlying architecture is based on the "Waterfall model". The development followed industry-standard quality attributes such as usability, navigation, accessibility, scalability, reliability, interoperability, maintainability, security, and conforms to the

standards of layered software architecture. The model ODIS (Fig. 2) has tried bridging the gap from perception to expectations of defence community/professionals.

Security features in ODIS

A centralized system often fails to ward-off external intrusions, identify theft, masquerading and securing participatory collaboration. The security of single 'sign-on' and access to restricted information for secure collaboration, communication, and sharing of information remains a concern in a centralized system. The model ODIS, which is a centralized system, offers inherent security for knowledge storage/safety/sharing, data provenance, data integrity and protection of intellectual property rights, etc.

To ensure the safety of information, the ODIS has incorporated security features such as CAPTCHA, email address, Mobile Number, IP address, unique record ID and Password. Besides, "it is compatible with the Open Web Application Security Project (OWASP) standards (2014)" with reference to Web Application Audit and free from other known vulnerabilities (Fig.3). However, vulnerability due to centralization remains. Therefore, using "blockchain" for the overall improvement of the ODIS system and contents hosted and the privacy of a contributor is studied in detail.

Discussion

The study discusses how to ensure the security, authenticity, and provenance of the content hosted on model ODIS and the contributors' privacy was among other concerns. The present study provides a proposed solution for model ODIS based on blockchain technology, but before that, four research questions have been explained in the following sub-paragraphs.

Research Question 1:What are the problems with the ODIS and similar online systems?

ODIS is a traditional centralized online system. The key is building a "trust"- trust for platform/device and trust for information, i.e., authentic and

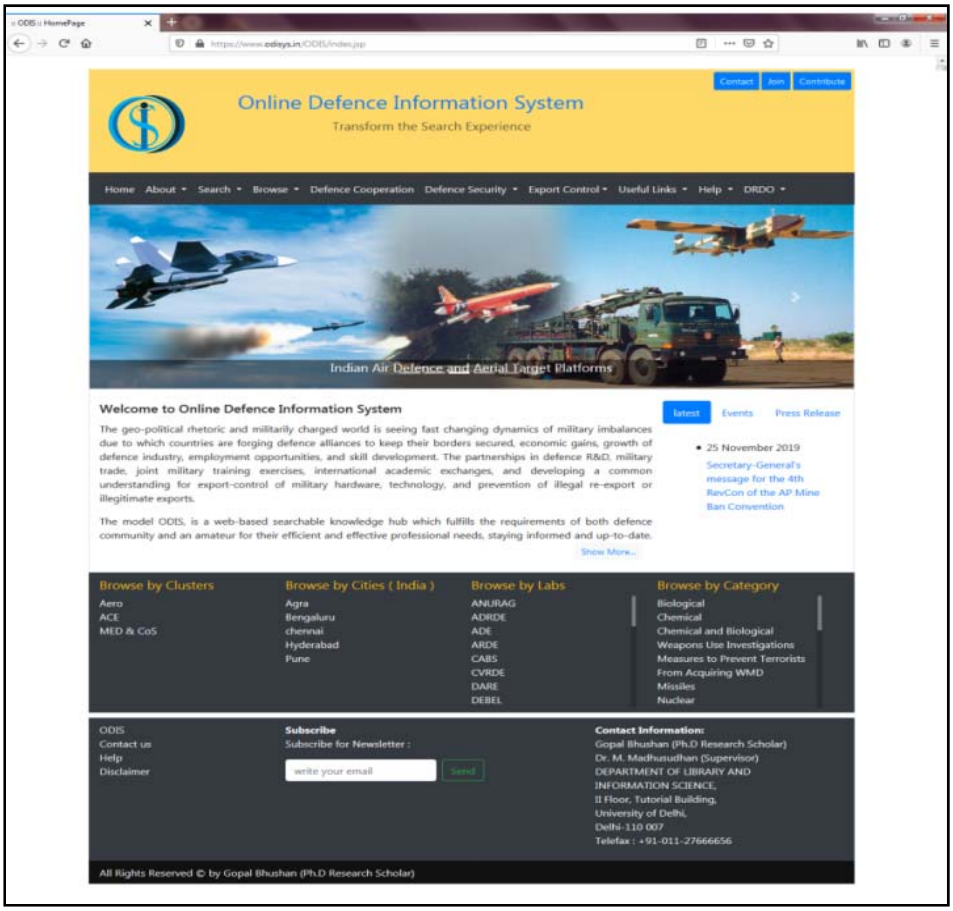

Fig. 2 — Snapshot of the homepage of ODIS (https://www.odisys.in)

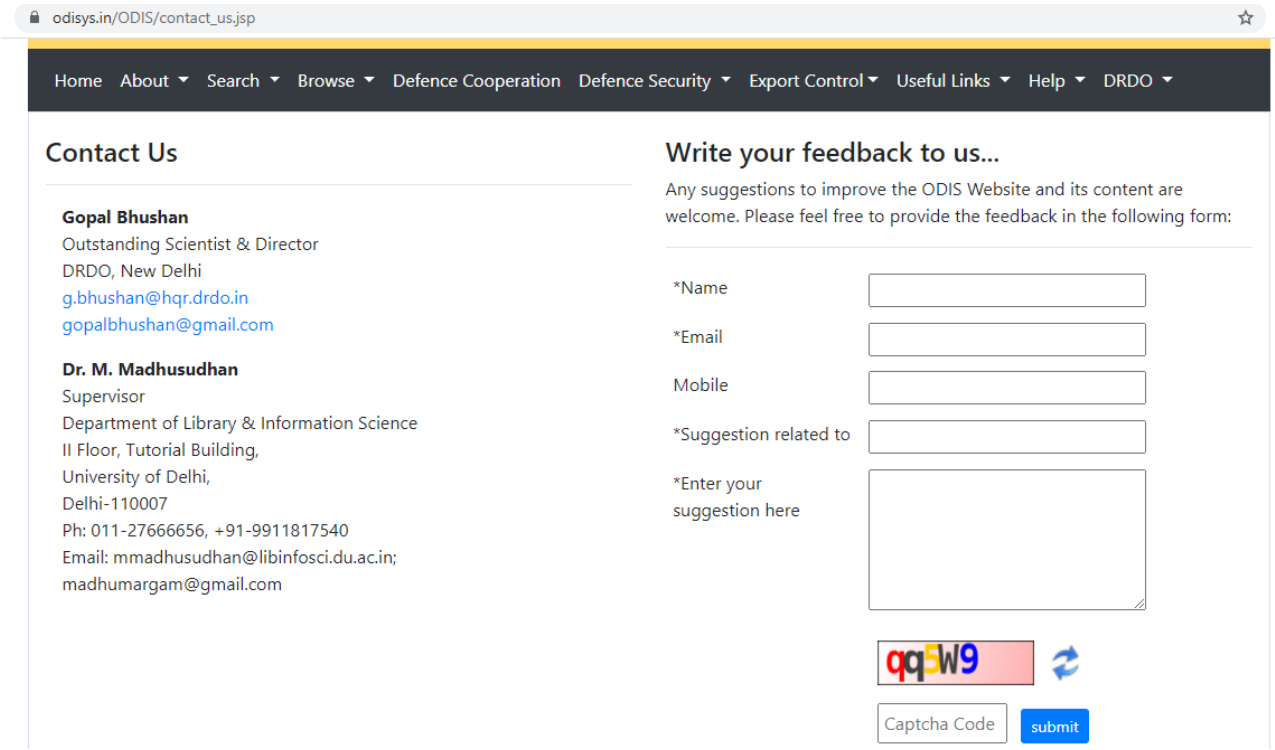

Fig. 3 — Snapshot of security features in ODIS (https://www.odisys.in/ODIS/contact_us.jsp)

verifiability. The enormity of tasks rests with managing the trust for a generation, storage, sharing, protecting, authentication and verifiability of a variety of knowledge sources being used/provided on ODIS and the authenticity of credentials of registered users. If ODIS scope were enhanced as a resource aggregator or virtual space provider, the trust, robustness and data integrity[20]would need further strengthening.

Research Question 2:What are the alternatives for effective cyber security?

The alternatives are (i) adopting a centralized cyber security protection scheme, where the underlying system of knowledge sharing remains the same. Still, an effective cyber security layer was implemented over it. This approach is prevalent in banking and financial sectors that have dedicated teams to supervise the security concerns but at a prohibitive cost; (ii) cloud-based architecture is achieved through decentralization and where security is implemented at different cloud layers. Similarly, there are a few other DLT models, prominent among them is blockchain, which at the core is a concept which inherently talks about proving the ownership and maintaining the ownership of data over a decentralized arrangement thus creating a peer-to-peer trust-based system without intermediaries[21].

Research Question 3: How to assure the safety and security of the tacit knowledge shared on ODIS?

In a conventional centralized system, the issue of collaboration, communication and sharing of information on a public platform is challenging and overwhelming. Such systems also need to ensure the rights of privacy of experts/contributors and protection of their credentials. Blockchain is revolutionary in this aspect; the owner of the data and consumer is connected without any intermediary, and if, there was an intermediary, it would be assistive (providing cloud space and other ancillary functions) in nature and not authoritative (the publisher portal has major control over the research data). Because of the decentralization of digital assets, the onus to prove data ownership remains with a contributor who proves the ownership of the data/digital asset without a centralized authority.

Research Question 4: How to counter the challenges of knowledge storage and sharing in the public domain?

Blockchain is a distributed, programmable and encrypted database that transfers, protects, stores, and quickly access knowledge from one location to another with high-security encompassment[22]. Blockchain ensures the authenticity of the uploaded documents/contribution and protects the provenance

and integrity of metadata. When information is stored in the blockchain, it is no longer possible to rewrite and modify it. The design makes blockchain capable of having a permanent historical record. It is a backward linked and cryptographically secured database not located on any server but distributed to all computers connected on the network[23]. Blockchain acts as a general ledger for registering records and reports. Because of its encryption and registration on all network computers, the recorded statements cannot undergo mutation, deletion or hacked[24]. A user can update information[25]. One of the main features of blockchain is intelligent contracts or smart contracts[26]. A smart contract is similar to data in the blockchain, which is distributed/replicated across a network; even if an attacker changes the smart contract of a node, the other nodes have a previous copy and deny the execution of transactions performed by the modified smart contract[27].

ODIS and blockchain for knowledge management and sharing

The model ODIS is designed and developed to provide information in the field of defence in the public domain, largely to the defence community[28]. Blockchain, through decentralization, offers a mutually trustable storage facility for information transacted between multiple users. The sharing of data/knowledge is done in parts of blocks. Each user acts as a node on the network and a data storage and mining server or a validating node. The content is stored in the form of blocks, and each of these blocks contains a hash which holds the fingerprint of the content. The hash of the next block contains the hash block of the previous one. The slightest change in the information of a block changes the hash characteristics[29]. If a person needs knowledge/content access/verification/traceability, all previous transactions related to this knowledge/content are made available, and linkage to the actual data is rendered. Fig. 4 shows the block diagram of a blockchain application in knowledge management processes.

In knowledge management, there are three core processes; knowledge creation/contribution, knowledge storage and knowledge sharing. The information management concept like IAM, data provenance and data integrity, and internal blockchain-based reward system are used to protect the IP and encourage the knowledge contributor. Fig.4 shows the hybrid architecture of ODIS on which knowledge management processes would interact. The two-way interaction, i.e., knowledge generation, deploying/ sharing and storing with blockchain's organizational knowledge, would increase speed to access and integration with blockchain-based knowledge management processing model[30].

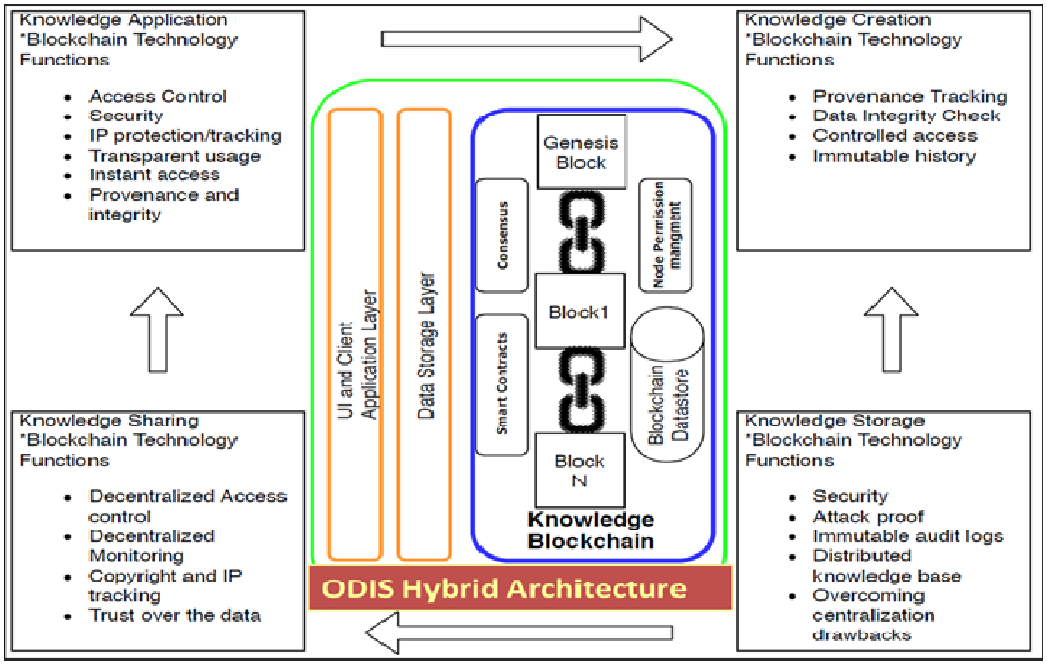

Fig. 4 — Conceptual model of blockchain
Source: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0177576, (Accessed on 17/5/2020)[29]

Blocks of ODIS using blockchain

Knowledge creation

With the help of blockchain, knowledge can be integrated and verified collectively[31]. Knowledge created can be sent to a blockchain verifiable database and made fully transparent for data/content provenance and integrity checks. Fig.5 depicts the knowledge creation concept.

ODIS data/content provenance and integrity services using blockchain

Blockchain provides the concept of "provenance", which is an efficient way of tracking the data with their ownership and helps in verifying the data that it had not been modified or altered. As ODIS aggregates the knowledge in the form of content provided by the developer and shared/uploaded by a contributor, it is vital to ensure that content/data uploaded/contributed is verifiable and not manipulated/morphed. To illustrate the concept, consider a news article published in 2001(old articles are usually archived or backed up on servers) on a news website and become viral in the year 2021. This is a possible scenario in which a hacker might get hold of this piece of news from a backed-up/archived server, alters the content and made it viral, possibly due to the absence of inherent provenance, data integrity, and traceability and authentication checks. This kind of content provenance and integrity traceability leads to the concept of "proof of ownership or origin". In a centralized data storage and retrieval system, as shown in Fig.6, a centralized system has been depicted to be acting as a single point of failure. In the model ODIS, it is proposed to incorporate data provenance and integrity traceability and authentication mechanism using blockchain for reaping the benefits of decentralization/distribution.

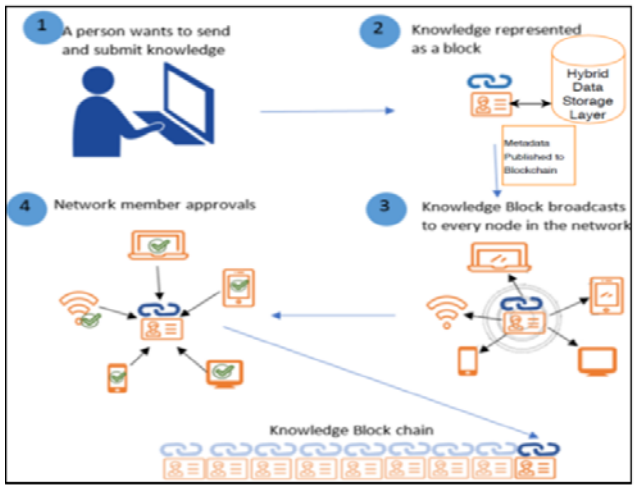

Fig.5 — Knowledge creation process at high level
Source: https://epub.uniregensburg.de/37703/1/TrustBus.pdf (Accessed on 15/5/2020)[32]

Proposed solution for model ODIS

A hybrid architecture based on blockchain is proposed using legacy systems for data storage and retrieval with secure and hack-proof traceability and authentication mechanism. In Fig.6, data provenance and data integrity are divided into three main services "Prov Recorder", "Prov Manager", and "Integrity Tracker". These three major services are smart contract layers or automated codes on the blockchain network, which get invoked at the start of the knowledge/content creation process (Fig.7).

(a) **Prov Recorder**: A smart contract layer is directly coupled to the storage/data layer and records any operation/history on the data items.

(b) **Prov Manager**: This service manages the data captured and published by the Prov Recorder service.

(c) **Integrity Tracker**: This service utilizes the blockchain stored provenance data and XML metadata to build a complete provenance chain and traceability. The prover's public key is used to encrypt the data, which is sent by a verifier and decrypts it with its private key. The prover has to prove the asset's ownership by proving the secret key, which matches the public key used to lock the asset[34].

Storing knowledge in ODIS using blockchain

Blockchain technology helps transactions stored in a decentralized manner and, in a way, transparently visible at any point in time[35]. Blockchain prevents conscious or unconscious changes. The system distributes the data in categories such as, "unencrypted data": data that can be read by any

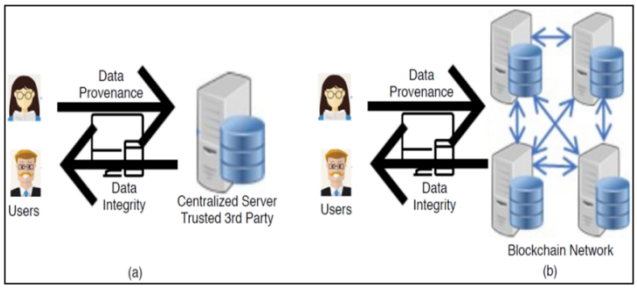

Fig. 6 — Data Provenance and integrity system approaches

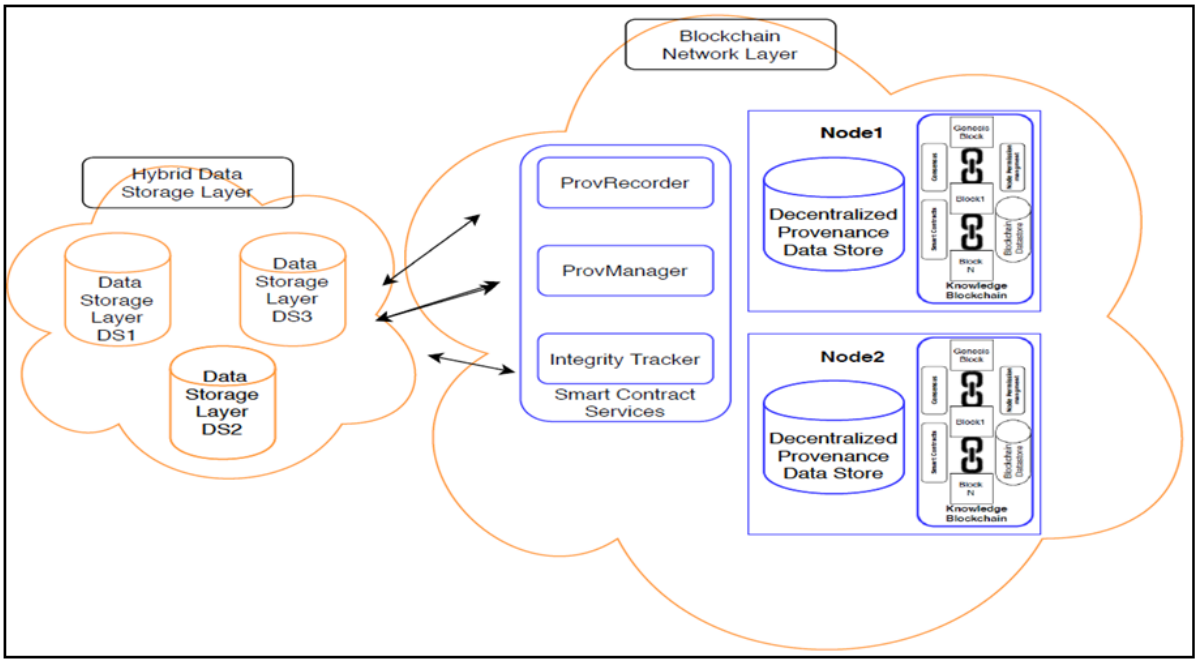

Fig.7 — Black-box architecture of provenance-based data integrity services
Source:https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0177576, (Accessed on 15/5/2020)[33]

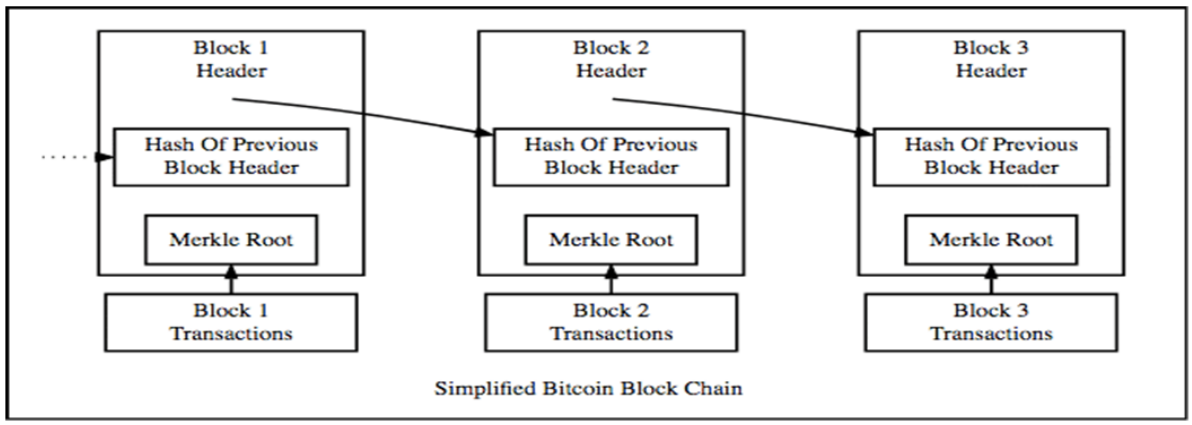

Fig.8 — Blocks connected to previous blocks by a cryptographic hash
Source: https://www.researchgate.net/figure/Simplified-Blockchain-Source Bitcoinorg2015 _fig1309414363(Accessed on 16/5/2020)[38]

blockchain or a general user; “encrypted data”: data that can be read by a user having access to the special decryption key (accessible via smart contracts); and, “hashed data”: data that was created in line with the function and such data cannot be manipulated as shown in Fig.8. The blockchain hashes are pre-stored and unloaded combined with the main data or metadata, creating a digital fingerprint of every transaction/action or data in the system. The lack of exhaustive, authentic data at any one point may have consequences, especially in exigencies. Following blockchain, the shared knowledge stored in ODIS would make all entities to come together to obtainthe benefits of authentic and cross-checked information[36] metadata is used to verify the actual data, a mismatch at any step is likely to cause errors. In traditional systems, data and metadata are stored on centralized servers. Using blockchain, these two entities can be separated and stored in a decentralized manner for better security and high availability[37].

Sharing of knowledge in ODIS using blockchain

The advantages of blockchain include high-speed information transfer, instant access and information security. Knowledge management challenges are “sharing of knowledge” and issues of intellectual

property rights or copyrights of knowledge shared. One of the important attributes of the blockchain database is that it deals with history in itself and is often called invisible. It is profoundly tricky (almost impossible) procedure to change the data in blockchain databases, which amounts to changing the information at all the nodes after that node. Therefore, it is a better and stronger reporting system[39] where knowledge sharing is more trustworthy due to robust security and the absence of a single point of failure. Each node has a copy of the original data, making ODIS a trustworthy and authentic platform to share the knowledge.

Identity and Access Management (IAM) services using blockchain

It is acknowledged that centralized knowledge management platforms/portals are characteristically hackable, and subscribers' data a potentially be published in the public domain. For ODIS, the blockchain-based decentralized IAM scheme would provide three main components (i) "identity provisioning"- update, revocation and lookup as these are a core set for identity management operations; (ii) "access control" for the prevention of unauthorized access to enterprise resources and for preserving the confidentiality of data; and, (iii) "monitoring and logging" to store and trace information is secured and auditable manner. Fig. 9, summarizes these three main functions of IAM. Since users on ODIS would have different privileges, signature chains can be utilized to make individual blockchains, which would make it easier to track the recording of documentation and screening/auditing of data and users and the option of changing the rights of users as and when needed. This reduces cost and enhances accuracy. In blockchain-enabled ODIS, each event would be recorded as a transaction, and contributors could have their content shared and re-shared and build a chain of trust.

Implementation of IAM over Blockchain

To implement IAM over blockchain, the core data related to "identities", "access control," and "logs"is implemented in a decentralized manner, as shown in Fig.10.

(a) ***Identity Management*:** Performs the functions of identification and authentication of each user and devicestored/marked on the blockchain network.

(b) ***Access Control***: Role-based policies are maintained in smart contracts over the blockchain network.

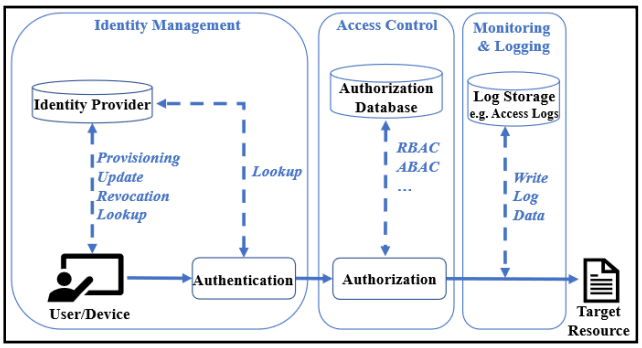

Fig.9 — Overview of IAM
Source: https://epub.uni-regensburg.de/37703/1/TrustBus.pdf, (Accessed on 15/5/2020)[40]

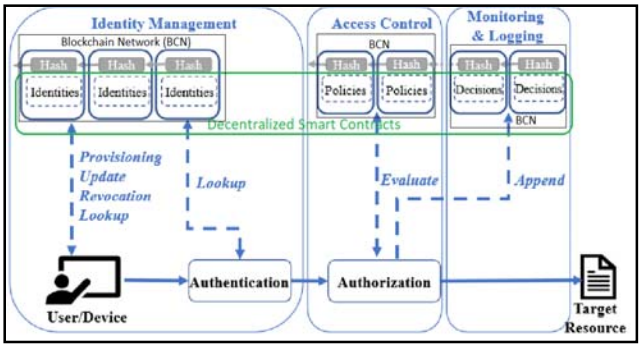

Fig.10 — Blockchain-based IAM
Source:https://epub.uni-regensburg.de/37703/1/TrustBus.pdf, (Accessed on 15/5/2020)[40]

(c) ***Monitoring and Logging***: Every activity to access the database is logged as a transaction that provides an immutable audit history. Usually, the audit logs and monitoring logs are kept in a hybrid storage layer where only the digital fingerprint is immutably stored and tracked. In a blockchain-based IAM system, many times, entire data rests in the blockchain, and thus the speed of the access may get impaired. Therefore, a clear distinction is needed as to what should go into blockchain and what should not.

Conclusion

The risks to–date on the internet have grown exponentially due to the complex nature of the computing environment in which data exists. Databases and servers need protection from external and internal intrusions. The confidentiality of contributors and customers is protected; data theft, data tampering, masquerading identity, and distributed denial of services have to be countered. The threat to data over the network has to ensure data

integrity, authenticity, and verifiability is keys to data protection and security concerns.

ODIS, in its present form, is based on a client/server architecture, which on receiving a request from users serves the requests from a central server to which requests are sent, and the server responds. The centralized system is based on Client-Server architecture. The central node that serves the other nodes in the system is the server node, and all the other nodes are the client nodes. The proposed model ODIS using blockchain technology would ensure security-related attributes; protection to databases and servers on which they reside; protection of the rights and preserving the confidentiality of registered users, and making ODIS a take away what it has promised to deliver.

The paper analyzes in detail the blockchain technology and its implementation methodologies with sufficient demonstrable illustrations. Blockchain is the best alternative, a technology that offers a secure way to record, share, store, and redistribution of information, establish provenance and traceability of ownership and offer hosts of features that would make ODIS a trustworthy platform. No denial of enhanced computational power has also brought proportional threats. The future lies in making "quantum-safe" applications that could withstand the attacks and threat of the order of quantum computational power. The developments in Extended Reality (XR) and Artificial Intelligence (AI)are further in future alternatives to make the ODIS NG (next generation) a quantum-safe and AI-XR enabled.

References

1 Porras J, Hiirsalmi P and Valtaoja A, Peer-to-peer communication approach for a mobile environment, *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 2004, DOI: 10.1109/HICSS.2004.1265717.

2 Forouzan B and Sophia CF, TCP/IP protocol suite , McGraw-Hill Education, 2007, pp. 866.

3 Bryant J and Pribanic-Smith E, Client server architecture using internet and public switched networks, Official Gazette of the United States, 1228 (5) 1999.

4 Charles R, Berger M E, David R and Ewoldsen R, A historical overview of research in communication science, The Handbook of Communication Science, 2010.

5 Elisa N, Yang L, Chao F and Cao Y, A framework of blockchain-based secure and privacy-preserving E-government system, Wireless Networks (2018). https://doi.org/10.1007/s11276-018-1883-0.

6 Miles C, Blockchain security: What keeps your transaction data safe? Available online: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/ (Accessed on 12/12/2020).

7 Lage O, de Diego S, Urkizu B, Gómez E and Gutiérrez I, Blockchain Applications in Cybersecurity, Computer Security Threats, 2019. DOI: 10.5772/intechopen.90061.

8 Nakamoto S, Bitcoin: A Peer-to-Peer Electronic Cash System, (2009) [Online]. Available: https://bitcoin.org/bitcoin.pdf.

9 Tran B, Lu Q and Weber I, Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management, *Proceedings of 16th International Conference on Business Process Management*, (2018) 56-60.

10 Yaxian J, Junwei Z, Jianfeng M, Chao Y and Xin Y, BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, *Journal of Medical System*, 42 (2018) 147.

11 Holotescu C, Understanding Blockchain Opportunities and Challenges, Proceedings of eLearning and Software for Education (eLSE), 4 (14) (2018), 275-283. DOI: 10.12753/2066-026X-18-253.

12 Daniel T, Bowen Z, Yuchen Y, Chenli C, and Haoran M, Blockchain applications in food supply information security, *Proceedings ofIEEE International Conference on Industrial Engineering and Engineering Management (IEEM 2017)*, (2017) 357-1361.

13 Beck R, Avital M, Rossi M and Thatcher J B, Blockchain technology in business and information systems research, *Journal of the Association for Information Systems*, 20 (9) (2019) 1388-1403.

14 Rossi M, Mueller-Bloch C, Thatcher J B and R. Beck, Blockchain research in information systems: current trends and an inclusive future research agenda, *Journal of the Association for Information System*, 20 (9) (2019) 1388-1403.

15 Arvind N, Joseph B, Edward F, Andrew M, and Steven G, Bitcoin and crypto-currency technologies: a comprehensive introduction, Princeton: Princeton University Press, 2016.

16 Wood G, Ethereum: A secure decentralisedgeneralised transaction ledger: byzantium version, Ethereum Project Yellow Paper. Available online: https://ethereum.github.io/yellowpaper/paper.pdf, (Accessed on 15/5/2020).

17 Hyperledger project, 2015, https://www.hyperledger.org. (Accessed on 15/5/2020).

18 Tian F, An agri-food supply chain traceability system for China based on RFID & blockchain technology, Proceedings *of 13th International Conference on Service Systems and Service Management (ICSSSM)*, (2016) 1-6.

19 GeeksforGeeks (2019). Available online: https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/ (Accessed on 15/5/2020).

20 Boehm W, A spiral model of software development and enhancement, *Computer*, 21 (5) 61-72.

21 Chowdhury J W, Colman A, Kabir M A, Han J and Sarda P, Blockchain versus database: A critical analysis, *Proceedings of 17th IEEE International Conference on Trust, Security and Privacy Computing Communication*, August 2018, pp. 1348-1353.

22 Onder I and Treiblmaier H, Blockchain and Tourism: three research propositions, *Annals of Tourism Research*, 2018. DOI: 10.1016/j.annals.2018.03.005.
23 Xu Z and Zheng H, Blockchain based medical records secure storage and medical service framework", Journal of Medical Systems, 43 (1) (2018). DOI: 10.1007/s10916-018-1121-4.
24 Savelyev A, Copyright in the blockchain era: promises and challenges, National Research University Higher School of Economics, Basic Research Program, Series: Law, 2017.
25 Oh J Sand Shong I, A case study on business model innovations using Blockchain: focusing on financial institutions, *Asia Pacific Journal of Innovation and Entrepreneurship*, 11 (2017) 335-344, DOI: 10.1108/APJIE-12-2017-038.
26 Ahmed K, Miller A, Shi E, Wen Z and Papamanthou C, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, *Proceedings of IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016. DOI: 10.1109/SP.2016.55.
27 Han S, Yue Z and He D, Automatic detection of search tactic in individual information seeking: a hidden markov model approach, *Proceedings of International Conference*, Fort Worth, TX, USA, February 12-15, 2013, pp. 712-716. DOI:10.9776/13330.
28 Kuhlthau CC, A principle of uncertainty for information seeking, *Journal of Documentation* 49 (4) (1993) 339-355.
29 Conceptual Model of Blockchain. Available online: https://journals.plos.org/ plosone/ article?id=10.1371/ journal.pone.0177576. (Accessed on 15/6/2020).
30 Suttcliffe G and Ennis M, Towards a cognitive theory of information retrieval, *Interacting with Computers*, 10 (1998) 321-351, DOI:10.1016/S0953-5438(98)00013-7.
31 Pressman R S, Software Engineering: A Practitioner's Approach, McGraw-Hill, (2001) pp. 860.
32 Knowledge Creation Process at High Level. Available online: https://epub.uniregensburg.de/37703/1/ TrustBus.pdf¸(Accessed on 15/5/2020).
33 Black-box architecture of provenance-based data integrity services. Available online: https://journals.plos.org/plosone/ article?id=10.1371/journal.pone.0177576 (Accessed on 15/5/2020).
34 Defence Information Systems, Cranfield University. www.cranfield.ac.uk/academic-disciplines/defence-information-systems.
35 Zhang G, Li T, Li Y, Pan H and Depeng J, Blockchain-based data sharing system for ai-powered network operations, *Journal of Communication and Information Networks*, 3 (2018) 1-8.
36 Kshetri N, Blockchain's roles in making key supply chain management objective, *International Journal of Information Management*, 39 (2018) 80-89. DOI: 10.1016/j.ijinfomgt.2017.12.005.
37 Akhavan P and Namvar M, Developing blockchain knowledge management model (BCKMM): Beyond tradition markets, 19th European Conference on Knowledge Management ECKM 2018, Italy, 2018.
38 Blocks connected to previous blocks by cryptographic hash. Available online: https://www.researchgate.net/ figure/Simplified-Blockchain-Source Bitcoinorg2015 _fig1309414363. (Accessed on 15/5/2020).
39 Pilkington M, Can blockchain technology help promote new tourism destinations? The Example of Medical Tourism in Moldova, 2017.
40 Blockchain based IAM. Available online: https://epub. uni-regensburg.de/37703/1/TrustBus.pdf (Accessed on 15/5/2020).