JOURNAL OF APPLIED INTELLIGENT SYSTEMS & INFORMATION SCIENCES
VOL. 4, ISSUE 1, PP. 50-59, OCTOBER 2023.
Available at: https://journal.research.fanap.com/
DOI: https://doi.org/10.22034/JAISIS.2023.412311.1066

A HOMOMORPHIC BLOCK APPROACH TO BLOCKCHAIN AND CLOUD ERP IMPLEMENTATION

Arnold Mashud Abukari[1,*], Vivek Gupta[2], Jhansi Bharathi Madavarapu[3], Vijaya Kittu Manda[4]

[1] *Tamale Technical University, Tamale, Ghana*
[2] *Indian Institute of Management Lucknow, Lucknow Prabandh Nagar, India*
[3] *University Of Cumberlands, Williamsburg, Kentucky, USA*
[4] *PBMEIT, Visakhapatnam, Andhra Pradesh, India*

ABSTRACT
Cloud Enterprise Resource Planning (ERP) comes with security and confidentiality challenges in a complex and integrated business environment. Cloud ERP systems are explicitly centered around various business enterprises. The growth of businesses worldwide, coupled with the need to do real-time transactions between these businesses, has created the need for more interactions between the ERP systems for these enterprises. To create this new ecosystem of different enterprises, integrating Blockchain Technology with the Cloud ERP offers a new decentralizing approach to ensure the effective creation of this ecosystem. This research identifies the importance and benefits of integrating blockchain technology with Cloud ERP and highlights the security implications this integration may present. The research proposed a Homomorphic Block Approach to implementing Blockchain and Cloud ERP to ensure a secure Cloud ERP data transmission to designated cloud ERP nodes in the ecosystem. This research has contributed significantly to implementing Blockchain and Cloud ERP integration.

KEYWORDS: Blockchain, ERP, Proof of Work, Proof of Stake, Consensus Algorithm, Homomorphism, Cloud ERP, Cloud Computing

1. INTRODUCTION

Businesses across the globe are adopting a centralized and integrated business solution called Enterprise Resource Planning (ERP). According to Amini and Abukari (2020), the ERP is a vital component that organizations need to manage their operations. The ERP System centralizes and integrates all business units within an organization to ensure the organization's management has complete control over the operations of the organization. The reliable communication and synchronization of data in the ERP system reduces the chances of severe errors and data duplication and improves decision-making at the earliest.

Implementing the Enterprise Resource Planning (ERP) solution over the years has taken many forms depending on organizations' strategies. Caldwell (2020) outlines four (4) ERP implementation strategies commonly adopted. The four ERP strategic approaches, according to Caldwell (2020), are Big Bang, phased rollout, parallel adoption, and hybrid. Implementing the strategic approach depends on the organizational size, risk tolerance, return on investment (ROI), and cost.

Since the advances made in the world of Cloud Computing, ERP solutions providers have developed ERP solutions to work in the cloud computing environment. Enterprise Resource Planning systems with Cloud

* *Corresponding Author, Email: amashud@tatu.edu.gh*

RECEIVED: 19 AUGUST 2023; **ACCEPTED**: 18 OCTOBER 2023; **PUBLISHED ONLINE**: 20 OCTOBER 2023

Computing architecture are classified as Software As A Service (SaaS) in the cloud computing delivering service model (Amini and Abukari, 2020). The definition of a Cloud ERP System presented by Fisher (2020) is a system that runs on a cloud platform, allowing organizations to access the solution through the internet. The Cloud ERP Software is hosted by a cloud vendor who provides the software as a service. The cloud ERP solution provider is responsible for the operations of the software, the cloud ERP Data storage, infrastructure, and, to some considerable extent, the security (Fisher, 2020).

Eight (8) key benefits of Cloud ERP Software were outlined by (Fisher, 2020) as upfront infrastructure and operating cost, implementation speed, accessibility, scalability, upgrades, customizations, and agility. Security, compliance, disaster recovery, storage resilience, and access are others.

Despite the advantages and benefits of Cloud ERP, security and confidentiality of data have been serious concerns raised by researchers and clients of Cloud ERP solutions. In an attempt to find a solution to security concerns, Blockchain technology will be considered.

2. BLOCKCHAIN TECHNOLOGY

Banerjee (2018) explained Blockchain as a distributed ledger with a list of transactions shared among several computers rather than a central server. According to Banerjee (2018), the distribution of the data or ledger guarantees security and enhances transparency. In Blockchain Technology, the list of transactions is made public and available to all parties. The information in the distributed ledger makes it possible to trace every single transaction in the Blockchain. Blockchain technology is cryptography-based with immutable algorithms, making it impossible for any party to manipulate the distributed ledger, hence secured (Banerjee, 2018). Every transaction in blockchain technology is verified and validated by members of the blockchain network called Miners. The Miners use computers with software or their coding skills to validate and verify every transaction in blockchain technology. Blockchain Technology is classified as part of the broader family of Distributed Ledger Technologies (DLTs), as stated by Faccia and Petratos (2021). The Blockchain is also described by Ibanez et al. (2021) as a digital register with transactions grouped into blocks linked in chronological order and having cryptography that guarantees integrity.

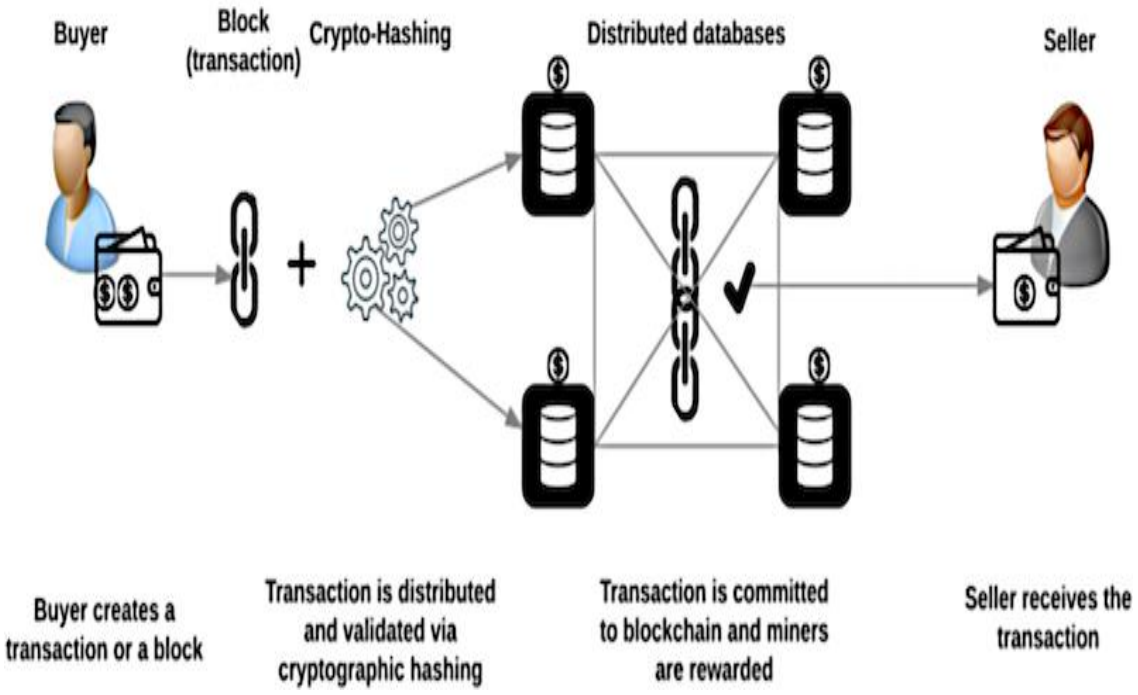

Fig. 1: Blockchain Process flow (Wikipedia, 2017)

3. BLOCKCHAIN PROTOCOLS

Blockchain technology is operated on a set of rules and guidelines. These sets of rules and guidelines are called Blockchain Protocols. Blockchain Protocols are the rules, guidelines, and algorithms designed to identify and control the operations of a network of Blockchains. According to Zhang and Lee (2019), blockchain protocols determine how data is stored and its transmission and validation across the entire network. This approach is geared towards ensuring the reliability, security, and consistency of the data generated through blockchain technology.

3.1. Blockchain Protocols Consensus Mechanisms

The consensus mechanisms of blockchain technology are one of the essential features of the blockchain protocols, which helps computers in the network to ensure transaction validity and the distributed ledger state. The most common consensus mechanisms in blockchain technology are the Proof of Stake and Proof of Work and the Byzantine Fault Tolerance mechanisms (Zhang and Lee, 2019). The Proof of Stake, Proof of Work, and the Practical Byzantine Fault Tolerance mechanisms are critical aspects of the blockchain protocol. Bitcoin uses the Proof of Work consensus mechanisms.

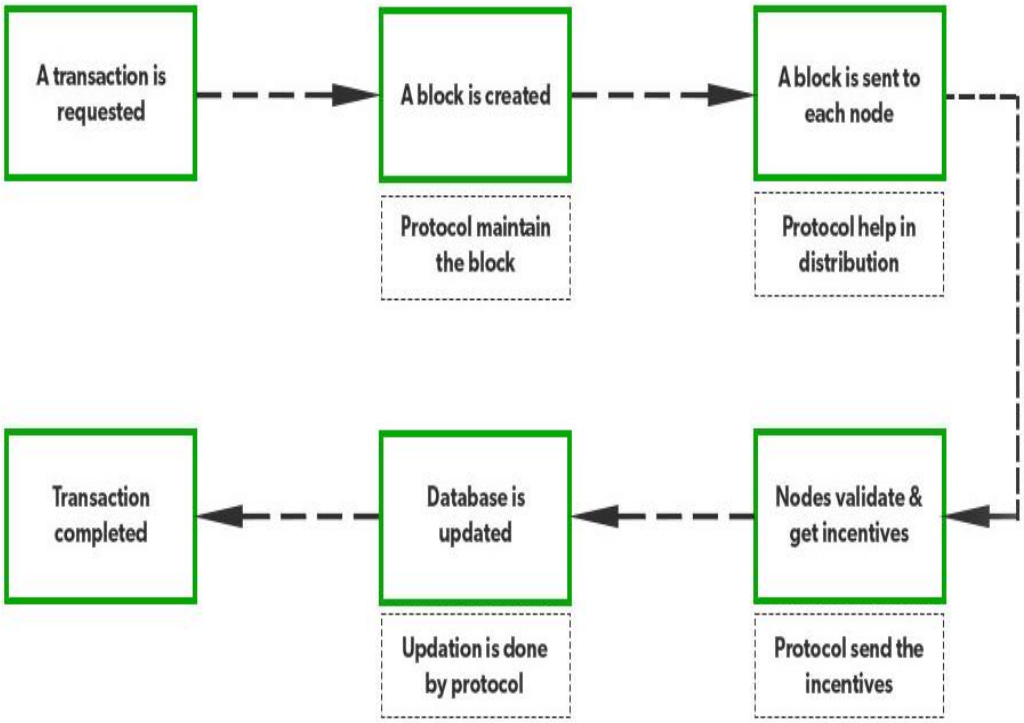

Fig. 2: Blockchain Protocols

3.2. Blockchain Protocols Cryptographic

In the wake of blockchain technology, industry leaders and researchers are concerned about the security and integrity of data generated. Blockchain protocols use cryptographic algorithms to ensure security and data integrity by creating unique digital signatures, public keys, private keys, and hash functions. The cryptographic algorithms are used to secure the network communication channels, identification, and authentication of all participating computers within the network.

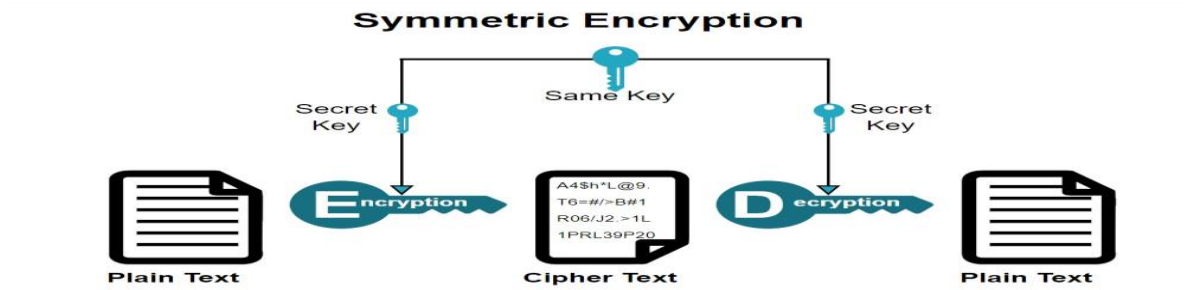

Fig. 3: Symmetric Encryption (Choudhary, 2023)

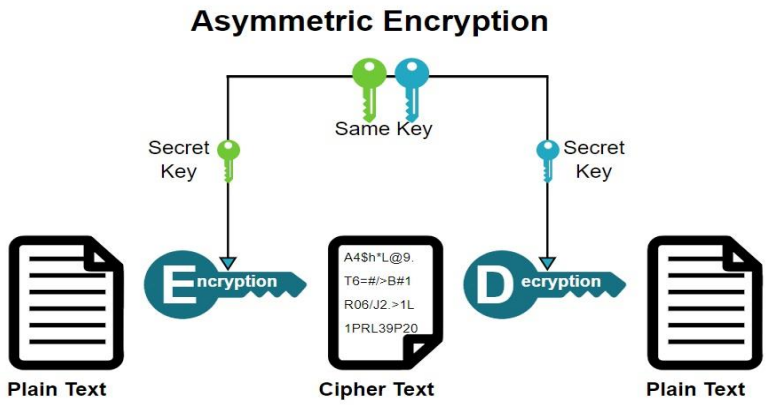

Fig. 4: Asymmetric Encryption (Choudhary, 2023)

3.3. Blockchain Protocols Smart Contracts

Some blockchain technologies like Ethereum support the Smart Contracts protocols approach. This approach of blockchain protocols is self-executing contracts with terms imbibed in the codes. The Smart contracts protocols ensure the rules are enforced, and penalties are meted out to deserving computers or users in the network based on the agreement without any intermediary.

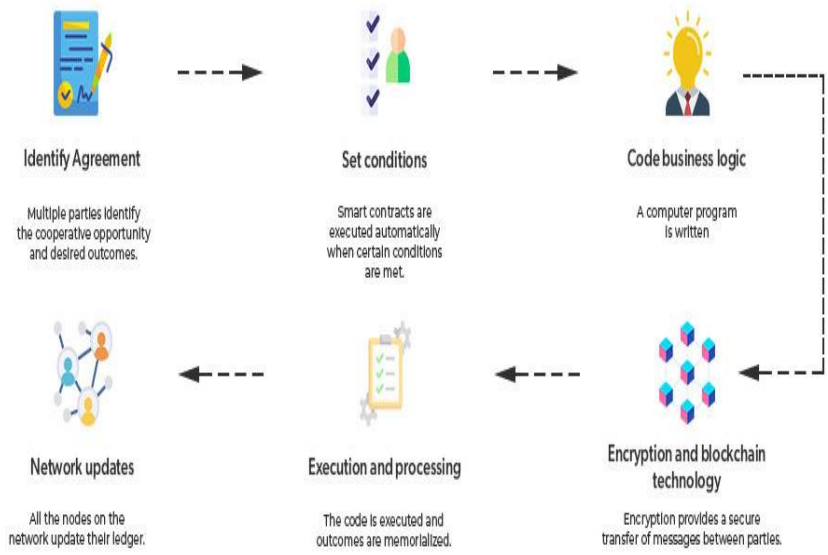

Fig. 5: Smart Contracts (Parikshit Hooda, 2022)

3.4. Blockchain Protocols Tokenisation

Creating the rules for the operations of the blockchain technology, managing digital representations of assets and tokens, rights or privileges within the network, and currencies are handled by the blockchain protocols tokenization in the form of tokens. The tokens concept ensures that transactions and ownership of real-world assets are adequately catered for. The tokenization process is represented in the Fig. 6.

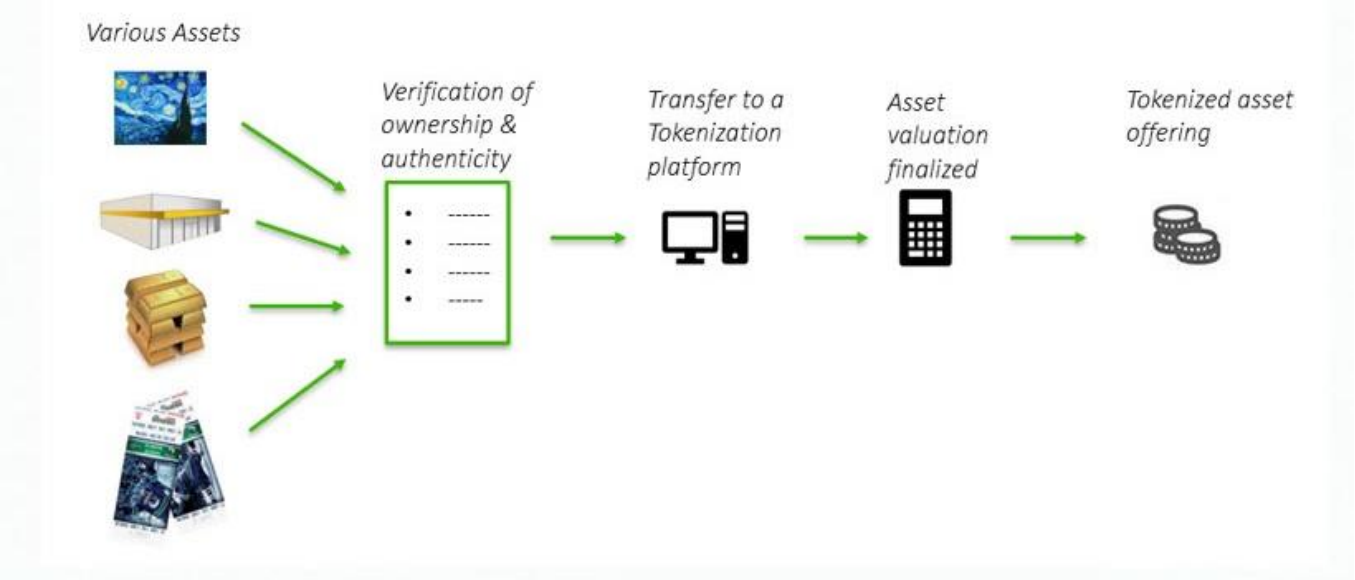

Fig. 6: Blockchain Tokenisation Process

4. BLOCKCHAIN CONSENSUS ALGORITHMS

Blockchain technology is a decentralized system that requires a particular algorithm or protocol for verification and validation. The key processes being handled by the consensus Algorithm is to set up a mechanism to verify, validate, and confirm transactions within the blockchain technology. The confirmed transaction is then recorded in an extensive distributed directory. The records of the transactions are known as block records (chain of blocks). These block records ensure the smooth implementation of the consensus protocols. Blockchain technology adopts several types of consensus algorithms. Notable among them are Proof of Work (PoW), Proof of Stake (PoS), Proof of Alternative (PoA), PBFT, Ripple, and DAC (Frikha et al., 2020).

4.1. Proof Of Work (PoW) Algorithm

According to Frikha et al. (2021), the Proof of Work (PoW) algorithm consumes much time and energy in the blockchain process. This has caught the attention of several researchers in the area of PoW algorithms worldwide. This research work also focuses on the Proof of Work algorithm. PoW creates a new block by selecting one node in every consensus round based on computational power. The first node to solve the problematic cryptographic puzzle or problem is allowed to create a block, as indicated in Fig. 7. The constant re-adjustment of the nonce of the nodes to solve the problematic cryptographic puzzle contributes significantly to increasing the computational power. The valid blocks in the chain increase as more puzzles are solved, accumulating more workload, making it difficult to overthrow a long chain due to computational power (Frikha et al., 2021). The PoW consensus approach is described by Frikha et al. (2021) as a Probabilistic-Finality consensus protocol.

4.1.1 Challenges with Proof Of Work (PoW)

Despite the remarkable security the PoW offers, it still has challenges that this research work considers worthy of discussing. Notable among the challenges are:

1) The 51% risk of controlling the network. If an entity has 51% or more of the nodes in the network, then the entity can control the majority of the network or corrupt the Blockchain.
2) The PoW Implementation is time-consuming since the miners may have to check many nonce values over some time to be able to solve a puzzle (Islam, 2022).
3) Miners consume many resources when the PoW is being implemented in the blockchain network. Solving the complex cryptographic puzzle essentially requires a high amount of computational power.
4) No real-time confirmation of transactions. The Proof of Work (PoW) consensus protocol transactions usually take 10 to 60 minutes for confirmation.

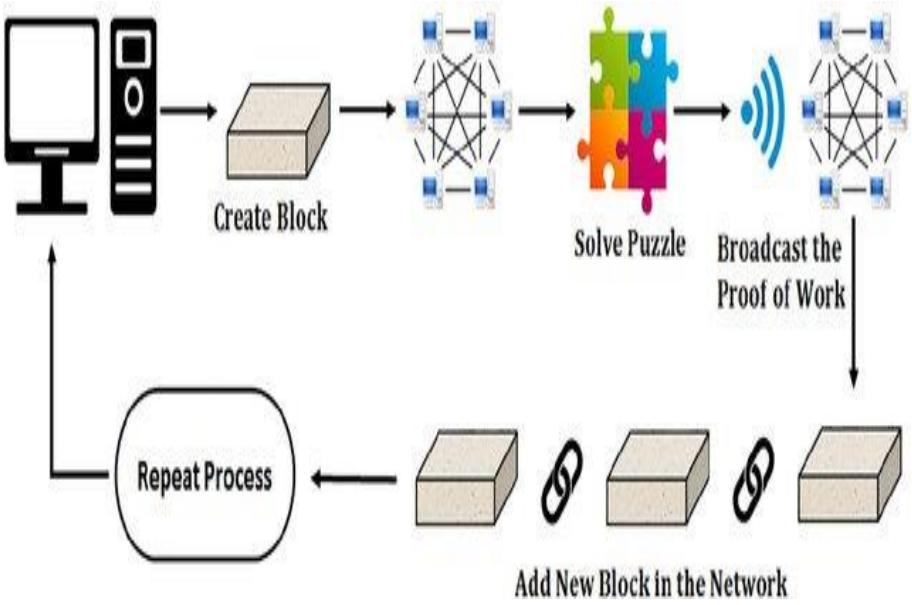

Fig. 7: Proof of Work (PoW) Process flow (Latif et al., 2021)

4.2. Proof Of Stake Algorithm

The Proof of Stake (PoS) Algorithm is one of the Blockchain consensus algorithms applied to reach consensus among the nodes in the blockchain technology. The Proof of Stake (PoW) is the second most adopted consensus algorithm used in the blockchain technology industry, and it continues to grow in numbers due to its low power consumption. The PoS algorithm uses stakes to create blocks, as presented in Fig. 8.

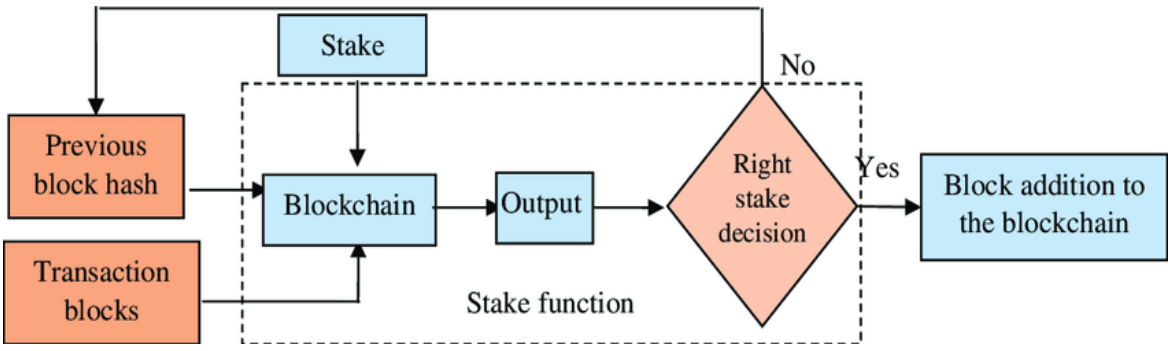

Fig. 8: Proof of Stake (Ananya et al., 2022)

5. Blockchain As A Service (BaaS)

The dream of every Enterprise Resource Planning (ERP) Service provider is to present a solution that can integrate all business processes (Hughes et al., 2020). In the quest of researchers and industry practitioners to effectively integrate ERP Systems by adopting blockchain technology, Blockchain As A Service (BaaS) was introduced. Blockchain As A Service (BaaS) is a platform built to implement the various components of Blockchain technology, such as smart contracts, a decentralized database, and nodes on the Cloud (Onik and Miraz, 2019). After conceiving the idea of the need for Blockchain-based ERP solutions, researchers in Zareravasan et al. (2020) argue. It will be challenging to extract a model for developing the blockchain-based ERP solution (Madavaarpu, 2023). Implementing blockchain technology on cloud ERP systems will add transparency and enhance the auditing of the transactions on the Blockchain enhanced Cloud ERP (Grover et al., 2018). Transaction validation and immutable records are essential benefits that can be tapped into when blockchain technology is implemented on Cloud ERP systems (Madavarapu & Yalamanchili, 2014).

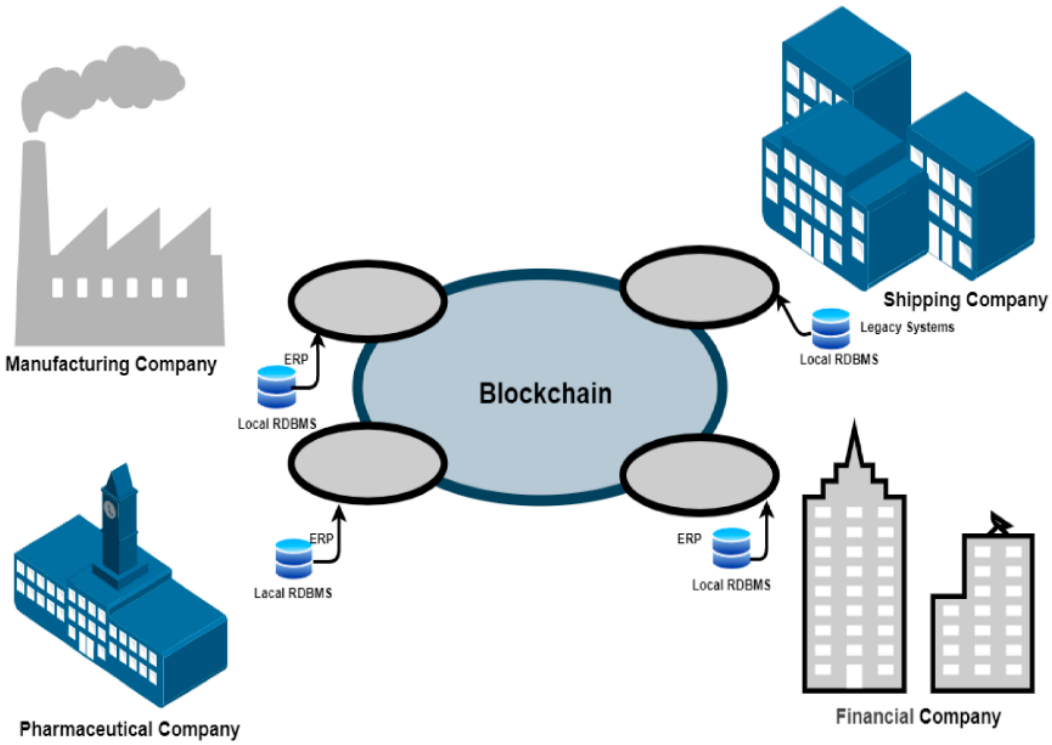

Fig. 9: The Role of Blockchain Technology and Cloud ERP (Kitsantas, 2022)

Uriarte et al. (2018) stated that monitoring and verification are handled by a third party based on a consensus mechanism or protocol called Proof of Concept (PoC). Kitsantas (2022) believes that implementing a blockchain-based cloud ERP system could be the next generation to reposition organizations effectively and securely (Madavaarpu et al., 2023). Cloud ERP systems or ERP systems from different geographical locations could be interconnected through Blockchain Technology, serving as a middleware (Sislian & Jaegler, 2022).

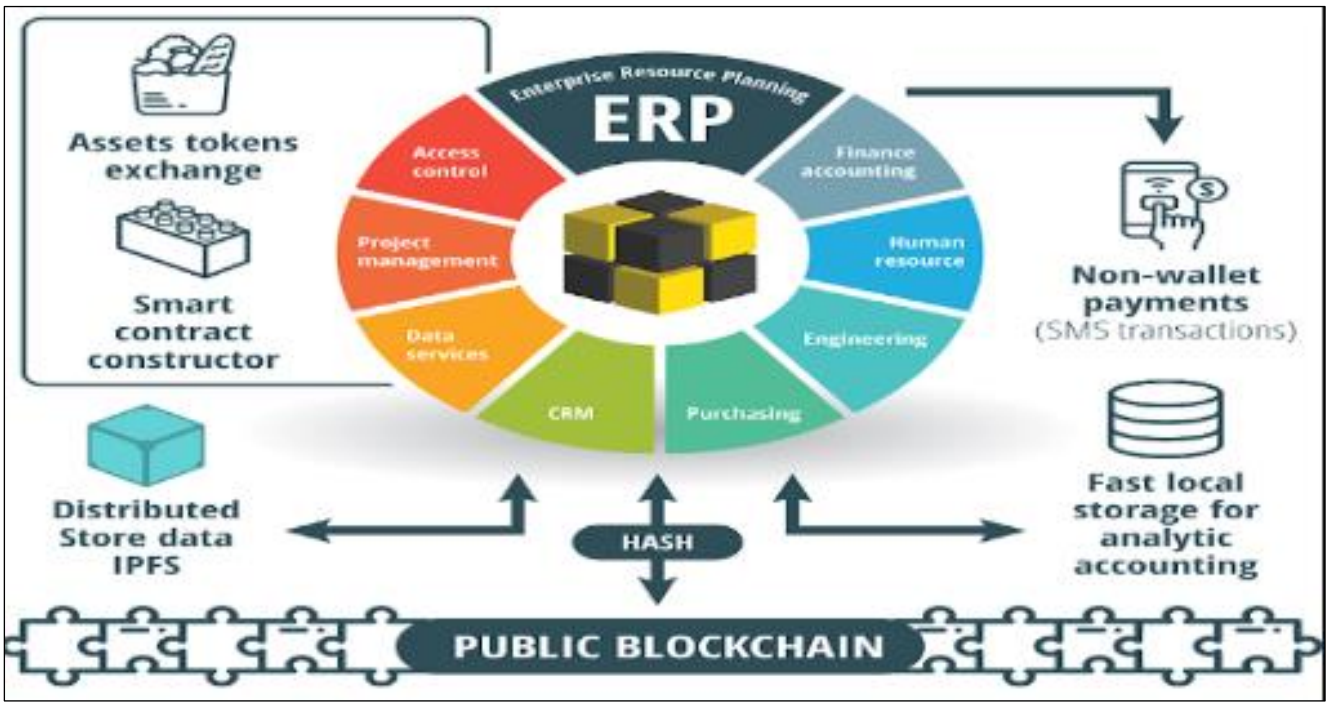

Fig. 10: Blockchain and ERP Implementation Relationship (https://www.linkedin.com/pulse/combinatorial-opportunity-blockchain-erp-sumit-kothiyal)

6. HOMOMORPHIC ENCRYPTION CONCEPT

To enable computation on encrypted data, homomorphic encryption was created. As a result, information can stay private while being processed, allowing for the completion of valuable activities using information from unreliable environments. Similar to other types of public encryption, a homomorphic cryptosystem encrypts data using a public key. It restricts access to its decrypted contents to those with the corresponding matching private key. However, its use of an algebraic structure to enable a range of computations (or operations) on the encrypted data distinguishes it from other types of encryptions.

6.1. Why Use Homomorphic Encryption

Organizations using conventional encryption techniques can secure sensitive data in cloud environments. However, they would need to either download and decode the material or examine or confirm the encrypted data if it were stored in the cloud. The first solution might result in security issues, while the second might be expensive and time-consuming. The actual benefit of homomorphic encryption becomes apparent in this situation. Thanks to homomorphic encryption, organizations can communicate confidential information to be reviewed securely and without compromising privacy. Organizations can use homomorphic encryption to perform mathematical operations on encrypted data without disclosing the actual data. With homomorphic encryption, only encrypted data is accessible to the cloud service provider, who may then use it to conduct calculations without first decrypting it. They could then give the owner of the secret data the encrypted results so they can decrypt them using a private key.

6.2. Proposed Homomorphic Block Approach for Blockchain and Cloud ERP

Researchers and industry professionals over the past few years have considered implementing blockchain-based Enterprise Resource Planning (ERP) systems. There have been several assurances regarding the improvement of security of the cloud ERP Data when implemented through blockchain technology. The critical question that motivated this research is, "What if I don't trust the blockchain?". This research proposes a Homomorphic approach to transmitting the blocks created for the blockchain nodes to operate on the homomorphic block without revealing the block's content to other Cloud ERP systems on the same Blockchain.

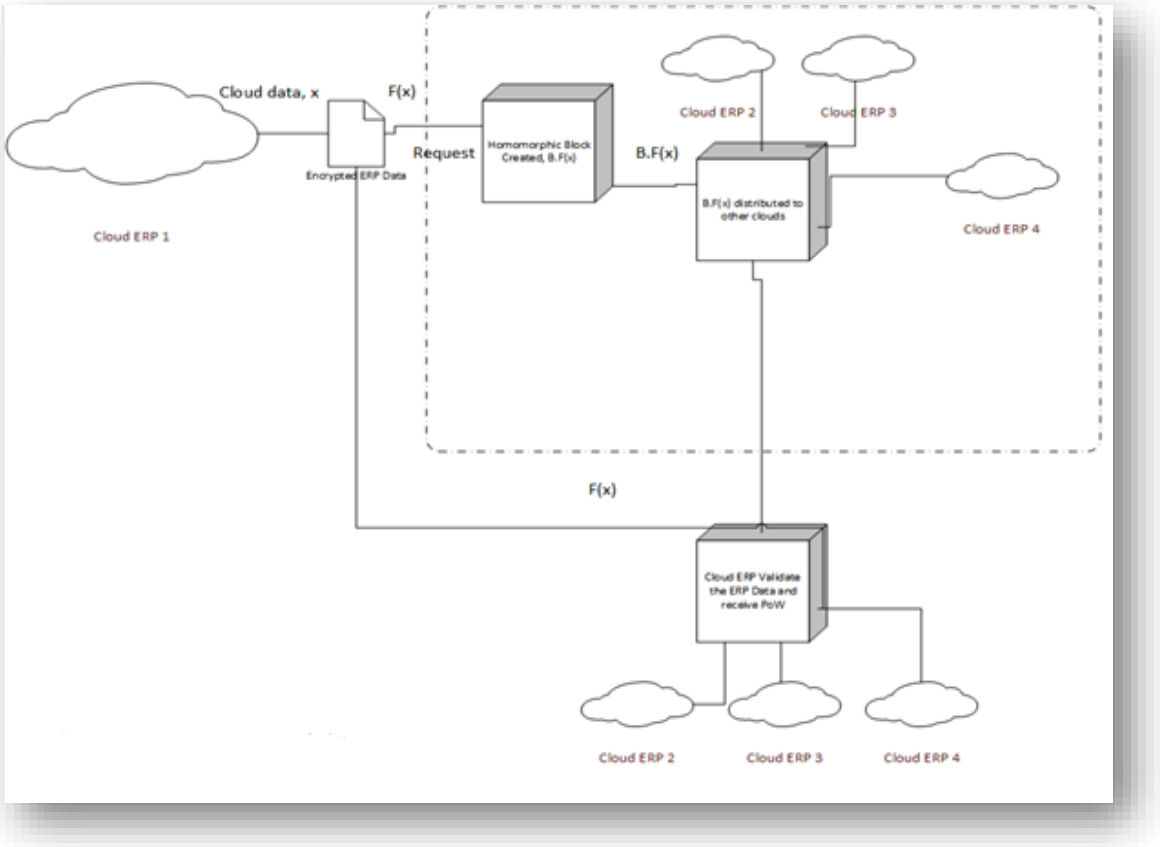

Fig. 11: Proposed Homomorphic Block Approach for Blockchain and Cloud ERP

Considering a Cloud ERP data *x* to be sent for transaction in the blockchain setup with other cloud ERP service providers. The cloud ERP data is first subjected to homomorphic encryption to generate a function f(x), which is then used to request a block.

$$f(x) = Enc\ (x) \qquad (1)$$

A block is created based on the f(x) as B.f(x) and sent to the designated cloud ERP in the Blockchain based on the address. The address of the designated cloud ERP is appended to the homomorphic function. Let the address of the Cloud ERP be B.

$$B.f(x) = Enc\ (x) * B \qquad (2)$$

Where B is the address of the intended Cloud ERP recipient. $B.f(x)$ It validates the Cloud ERP data used for the transaction and receives its Proof of Work (PoW). The encrypted data is sent to the originating cloud ERP to update its transaction blocks.

7. CONCLUSION

Based on the theoretical and conceptual point of view, this research has significantly contributed to the ongoing research in blockchain and cloud ERP implementation. The research has also highlighted the security implications of implementing blockchain-based cloud ERP when the Blockchain is not trusted. A comprehensive proposed homomorphic block approach is presented in this research to address trust issues in the implementation of blockchain-based Cloud ERP solutions in a multi-cloud environment. The research has also highlighted the importance of security enhancement, immutable records, consensus mechanisms, smart contracts, and tokenization. Blockchain-based Cloud ERP is new in research with so much potential since it presents a new dimension to decentralization and security enhancement in Cloud ERP Data.

REFERENCES

Amini, M., & Abukari, A. M. (2020). ERP systems architecture for the modern age: A review of the state of the art technologies. Journal of Applied Intelligent Systems and Information Sciences, 1(2), 70-90.

Banerjee, A. (2018). Blockchain technology: supply chain insights from ERP. In Advances in computers (Vol. 111, pp. 69-98). Elsevier.

Caldwell, A. (2020, August 8). 4 Key ERP Implementation Strategies. Oracle Netsuite. Retrieved October 19, 2021, from https://www.netsuite.com/portal/resource/articles/erp/erp-implementation-strategies.shtml.

Faccia, A., & Petratos, P. (2021). Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration. Applied Sciences, 11(15), 6792.

Fisher, K. (2020). What is Cloud ERP and How Does It Work?. Oracle Netsuite, 12.

Ibañez, J. I., Bayer, C. N., Tasca, P., & Xu, J. (2021). Triple-entry accounting, blockchain and next of kin: Towards a standardization of ledger terminology. arXiv preprint arXiv:2101.02632.

Islam, H., Madavarapu, J. B., Sarker, N. K., & Rahman, M. A. (2022). The Effects of Cyber Threats and Technical Problems on Customer's Attitude Towards E-Banking Services. Oblik i finansi, 96, 58-67.

Frikha, T., Choura, H., Abdennour, N., Ghorbel, O., & Abid, M. (2020). ESP2: embedded smart parking prototype. Advances in Science, Technology and Engineering Systems Journal, 5(6), 1569-1576.

Grover, P., Kar, A. K., & Vigneswara Ilavarasan, P. (2018). Blockchain for businesses: A systematic literature review. In Challenges and Opportunities in the Digital Era: 17th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2018, Kuwait City, Kuwait, October 30–November 1, 2018, Proceedings 17 (pp. 325-336). Springer International Publishing.

Hughes, D. L., Rana, N. P., & Dwivedi, Y. K. (2020). Elucidation of IS project success factors: an interpretive structural modelling approach. Annals of Operations Research, 285, 35-66.

Latif, S., Idrees, Z., e Huma, Z., & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. Transactions on Emerging Telecommunications Technologies, 32(11), e4337.

Madavarapu, J. B. (2023). Electronic Data Interchange on Blockchain. Journal Homepage: http://www. ijmra. us, 13(07).

Madavarapu, J. B. (2014). Payroll management system.

Madavarapu, J. (2023). Electronic Data Interchange Analysts Strategies to Improve Information Security While Using EDI in Healthcare Organizations. Available from ProQuest Dissertations & Theses Global. (2832638159). https://www.proquest.com/dissertations-theses/electronic-data-interchange-analysts-strategies/docview/2832638159/se-2.

Madavarapu, J. B., Mohammed, F. H., Salagrama, S., & Bibhu, V. (2023). Secure Virtual Local Area Network Design and Implementation for Electronic Data Interchange. International Journal of Advanced Computer Science and Applications, 14(7).

Onik, M. M. H., & Miraz, M. H. (2019). Performance analytical comparison of blockchain-as-a-service (baas) platforms. In Emerging Technologies in Computing: Second International Conference, iCETiC 2019, London, UK, August 19–20, 2019, Proceedings 2 (pp. 3-18). Springer International Publishing.

Sislian, L., & Jaegler, A. (2022). Linkage of blockchain to enterprise resource planning systems for improving sustainable performance. Business Strategy and the Environment, 31(3), 737-750.

Uriarte, R. B., De Nicola, R., & Kritikos, K. (2018, December). Towards distributed sla management with smart contracts and blockchain. In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 266-271). IEEE.

Yalamanchili, R. K. (2014). International Student Portal.