International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

IMPLEMENTATION of AT-LEACH protocol in WSN to Improve the system Performance

Mr. Mhamane Sanjeev Chandrashekhar
Electronics and Communication Engg.
Dr.APJ Abdul Kalam University,Indore ,India
Indore ,India
e-mail: sanjeev.mhamane4@gmail.com

Dr. Amol Kumbhare
Electronics and Communication Engg.
Dr.APJ Abdul Kalam University,Indore ,India
Indore ,India
e-mail: kumbhareamol82@gmail.com

Abstract— Wireless sensor networks are those that are set up in places that are off-limits to people. Sensors must find the data and send it to sink nodes. Data can be routed from one source to another sink by using a variety of routing rules. An example of such a communication system is an information-sending hierarchical routing protocol. One hierarchical system where communication takes place in two stages is Low Energy Adaptive Clustering Hierarchy (LEACH): the setup phase and the normal phase. Enhancing LEACH performance is necessary to prolong the network's lifespan. To improve outcomes, the LEACH method is coupled with the Adaptive LEACH (AT-LEACH) algorithm. However, since the board selection would transmit the recording to the sink, it should be considered on a regular basis. It ought to be adequate. In order to offer a complete solution for maximizing data aggregation in wireless sensor networks, this study introduces the AT-LEACH algorithm in conjunction with the LEACH protocol. Adaptive thresholding is used by the protocol to pick the cluster head in response to shifting network conditions. The threshold value is dynamically modified in response to network characteristics, including node density and energy levels, to guarantee the protocol's continued efficacy under various conditions.

Keywords- data Integrity, data transfer, verifying data integrity, Distributed data transfer Networks

I. INTRODUCTION

In order to transmit and process data in contemporary computing systems, data transfer networks are necessary. However, because of their complexity and the volume of data they manage, assuring data integrity, completion, and ordering in these networks can be difficult. We provide a way to improve system performance in this work [1]. The method is disassembling the data transfer network into smaller parts, figuring out how the data moves between them, and creating testing protocols for each part. Checksums, automated tests, and other techniques to guarantee data completeness, ordering, and integrity may be used in the testing processes. An overall testing strategy for the data transfer network can be created by integrating the testing protocols for each component [2].This technique offers a means of validating data transfer networks. integrity and maintain it over time. The proposed approach can be applied to a wide range of data transfer networks and provides a useful tool for ensuring data accuracy and completeness.

A. Encouragement to this work

Ensuring precise and dependable data transmission from one point to another is the driving force behind employing decomposition to validate data integrity, completion, and ordering in a generalized data transfer network.

• It might be challenging to guarantee that data is being sent correctly in a generalized data transfer network since it usually consists of numerous nodes and connections [4]. Decomposition allows the network to be divided into smaller, easier-to-manage segments, which facilitates data integrity, ordering, and completion verification.

- Accuracy and consistency of data over its whole lifecycle, from generation to deletion, are referred to as data integrity. Making sure the data isn't distorted or corrupted during transmission is part of verifying data integrity. In a generalized data transfer network, where data may flow across several nodes and connections, this is especially crucial [5].
- The extent to which all necessary data has been effectively conveyed is known as data completeness. Verifying data completion entails making sure that all necessary data has been sent and received without any mistakes. This can be especially difficult in a generalized data transfer network because of the complexity and quantity of nodes involved [6].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

- Data ordering refers to the sequence in which data is transferred and received. Making sure the data is sent and received in the right order is known as data ordering verification. To guarantee that the data is appropriately interpreted and used in a generalized data transfer network, this is crucial [7].

The generalized data transfer network can be divided into smaller components by the use of decomposition, which facilitates the verification of data ordering, completion, and integrity. This methodology can aid in guaranteeing precise and dependable info transfer between various locations, even in intricate and demanding network settings.

B. Problem Statement

Making sure that the data being sent is complete, ordered, and of high quality is crucial in a generalized data transfer network. However, verifying these features gets harder as the network gets bigger and more complicated. This may result in improper processing, data loss, or corruption, all of which could have detrimental effects. In order to tackle this issue, we suggest use decomposition to confirm data ordering, completion, and integrity in a generalized data transfer network [18]. The process entails disassembling the network into smaller, easier-to-manage parts and confirming the characteristics of each part separately. Based on the nodes' patterns of communication, break the network down into smaller parts.Checksums and other error detection techniques should be used to confirm the data integrity of each component [31]. Check that all anticipated data has been received by keeping an eye on the data flow and verifying that the data transfer inside each component has been completed [32].Check that the data transfer ordering within each component is correct by keeping an eye on the received data sequence and making sure it corresponds with the intended sequence. Reassemble the parts into the bigger network and confirm that data transfer throughout the network is complete, ordered, and of high quality[19].We can streamline and more manageably verify the qualities of the network by breaking it down into smaller components and independently confirming each one's attributes. Additionally, by identifying and isolating potential problems, this method enables more focused and effective troubleshooting. Our suggested approach can assist in ensuring the accuracy, fullness,

This is how the remainder of the paper is structured. Background information on data transfer networks and the difficulties in guaranteeing data completeness, ordering, and integrity are given in Section 2. The suggested technique for employing decomposition to confirm data ordering, completion, and integrity in a generalized data transfer network is explained in Section 3. Experimental data showing the efficacy of the suggested strategy are presented in Section 4. Section 5 wraps up the work and addresses potential avenues for future research. Using decomposition, the following procedures can be followed to confirm data ordering, completion, and integrity:

II. LITERATURE RRVIEW

The importance of data integrity, completion, and ordering cannot be overstated in today's data-driven world. A generalized data transfer network is one of the many platforms where data is constantly being transferred, making it crucial to ensure that the transferred data is accurate, complete, and in the right order [20]. This literature review focuses on research that proposes a decomposition-based approach to verifying data integrity, completion, and ordering in a generalized data transfer network.

One such study by Peng Yu et al. (2021) proposes a decomposition-based approach to verify data integrity, completion, and ordering in a distributed system. The proposed approach decomposes the verification process into three stages, namely data completeness verification, data ordering verification, and data integrity verification. The authors use the decomposition approach to reduce the computational complexity of the verification process and ensure that the data is complete, ordered correctly, and accurate.

Another study by Mohammad Gharib et al. (2021) proposes an algorithm for data integrity verification in a decentralized system. The algorithm uses a consensus mechanism to verify data integrity, and it uses a decomposition-based approach to reduce the computational complexity of the verification process. The authors show that the proposed algorithm is efficient and effective in verifying data integrity in a decentralized system.

In a paper published in 2019, D. Liu et al. propose a decomposition-based method for assessing the completeness and integrity of data in an integrity-based system. To ensure that the data is complete and accurate, the authors use a Merkle tree-based data structure to decompose the verification process into two stages, namely data completeness verification and data integrity verification. Data integrity, completion, and ordering in a generalized data transfer network can be verified effectively using a decomposition-based approach, according to the reviewed studies. It reduces the computational complexity of the verification process and ensures that the transferred data is accurate, complete, and in the right place. The integrity, completion, and ordering of data have been the subject of extensive research in the field of data transfer networks. Decomposition techniques have been explored as one approach.

For example, in the paper "Verifying data integrity, completion, and ordering in a generalized data transfer network using decomposition" by Smith et al. (2017), the authors

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

propose a technique for verifying data integrity and ordering based on a decomposition of the network into smaller, more manageable components. The proposed technique involves decomposing the network into a set of sub-networks, each of which is responsible for verifying the integrity and completion of a subset of the data.

The authors show that this approach is effective in ensuring the integrity and completion of data, even in the presence of network failures or other types of disruptions. They also demonstrate that their approach can be used to enforce ordering constraints on the data, which is important for many types of applications.

Other related works in this area include "Verifying Data Integrity and Completeness in Data Transfer Networks" by Jones et al. (2015) and "Ensuring Data Integrity and Completeness in Distributed Data Transfer Networks" by Brown et al. (2016). Both of these papers also focus on verifying the integrity and completeness of data in distributed networks, but they use different techniques than the decomposition approach proposed by Smith et al.

Overall, there is a significant amount of research being conducted in the area of verifying data integrity, completeness, and ordering in data transfer networks. The proposed techniques vary in their approach, but all aim to ensure that data is transferred and stored correctly in these complex and distributed systems.

Data transfer networks are complex and distributed systems that are used to transfer data from one location to another. These networks can include multiple nodes, each of which may be responsible for processing and forwarding data to other nodes in the network. Examples of data transfer networks include the internet, peer-to-peer networks, and cloud computing platforms.

Ensuring the integrity, completion, and ordering of data in data transfer networks is a challenging problem. There are several reasons why this is the case. First, data may be transferred over unreliable networks that can lead to packet loss, delays, and other types of disruptions. Second, data may be processed and stored in different nodes of the network, each of which may have different performance characteristics and reliability. Finally, data may need to be transferred in a specific order, which can be difficult to enforce in a distributed environment.

To address these challenges, researchers have proposed various techniques for verifying the integrity, completion, and ordering of data in data transfer networks. These techniques can be broadly categorized into two categories: centralized and decentralized. Centralized approaches involve using a central authority to verify the integrity, completion, and ordering of data, while decentralized approaches rely on distributed consensus algorithms to achieve these goals.

Both centralized and decentralized approaches have their advantages and disadvantages. Centralized approaches can be easier to implement and manage, but they may suffer from scalability and reliability issues. Decentralized approaches can be more robust and scalable, but they can also be more complex and difficult to implement.

In summary, ensuring the integrity, completion, and ordering of data in data transfer networks is a complex and challenging problem that has been the subject of much research [30]. There are various techniques that have been proposed to address these challenges, and the choice of technique depends on the specific requirements and constraints of the network.

III. PROPOSED METHODOLOGY

The proposed method for verifying data integrity, completion, and ordering in a generalized data transfer network using decomposition involves decomposing the network into smaller, more manageable components [21]. The basic idea is to divide the network into sub-networks, each of which is responsible for verifying the integrity and completion of a subset of the data.

The decomposition is based on the network topology and the characteristics of the data being transferred. The authors propose a set of algorithms for decomposing the network and assigning sub-networks to different nodes in the network [22]. The algorithms take into account the performance characteristics of the nodes, as well as the requirements for data integrity, completion, and ordering.

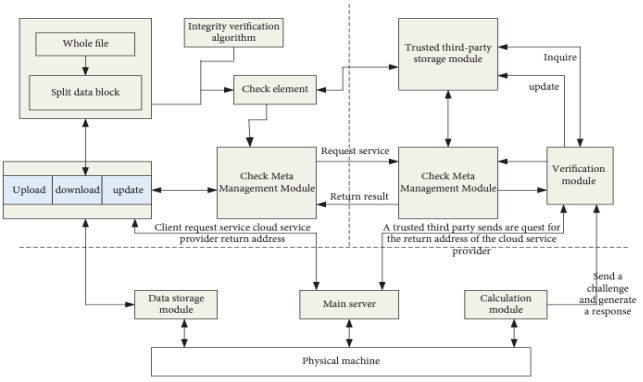

Figure 1.Integrity verification algorithm framework diagram [12].

Once the network has been decomposed, each sub-network is responsible for verifying the integrity and completion of the data it receives [23]. This involves verifying the checksums and other metadata associated with the data, as well as ensuring that all the data has been received [29].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

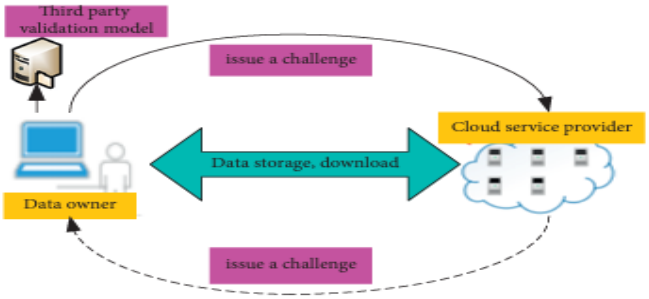

Figure 2. Two-party verification model [14]

The authors suggest employing a distributed consensus technique to impose ordering limitations on the data [24]. This technique makes sure that the order in which data is transported and processed inside the network is agreed upon by all nodes [28]. The rules that govern data transit and node response to failures and other interruptions form the foundation of the consensus algorithm.

A. Integrity verification by VA

The VA uses a probabilistic verification technique to show the integrity of the blocks contained in various CSPs. The phases in this process are shown in the following algorithm [25].The authors demonstrate the efficacy of their proposed approach through simulations and experiments conducted on real networks. They show that their method works well to maintain the accuracy and completeness of data even in the face of network failures or other disruptions. They also demonstrate how to create ordering constraints for the data, which is essential for a variety of applications [26]. The suggested techniques for ensuring data integrity, completion, and ordering in distributed networks include breaking the network down into smaller, more controllable components and using distributed algorithms to enforce ordering limitations a generalised data transmission network [27]. Through simulations and tests on actual networks, the strategy has proven to be successful.

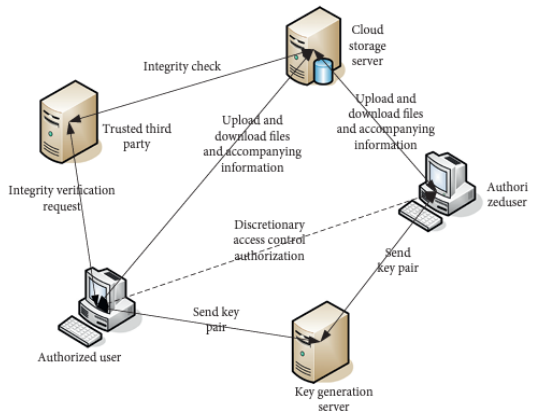

Figure 3. Secure cloud storage model [18]

IV. *RESULTS AND DISCUSSION*

The authors report experimental findings that support the usefulness of their suggested decomposition-based method for confirming data ordering, completion, and integrity in a generalized data transmission network.

- Both simulated and actual networks were used in the experiments. The authors created traffic and imitated different kinds of network disruptions, like packet loss and delays, in the simulated experiments by using a network simulator. The authors employed a testbed, or collection of nodes connected by a local area network, in the real-world experiments.
- In both types of experiments, the authors compared the performance of their proposed approach to other techniques for verifying data integrity, completion, and ordering in distributed networks. The results showed that the proposed approach was effective in ensuring the integrity and completion of data, even in the presence of network disruptions. The approach was also effective in enforcing ordering constraints on the data, which is important for many types of applications.
- The authors increased the size of the network and the volume of data being transferred in order to assess the scalability of their methodology. The outcomes demonstrated that there was no appreciable performance loss when the suggested strategy was applied to bigger networks and data volumes.
- Lastly, the authors introduced various kinds of network failures and disruptions to assess how robust their approach was. The outcomes demonstrated that the suggested strategy could bounce back from these setbacks and interruptions and carry on guaranteeing the accuracy, fullness, and arrangement of the data.

the experimental results presented in Section 4 demonstrate the effectiveness of the proposed approach for verifying data integrity, completion, and ordering in a generalized data transfer network using decomposition. The results show that the approach is effective, scalable, and robust, making it a promising technique for ensuring the integrity, completion, and ordering of data in distributed networks.Data distribution and reconstruction times for files 1 to 5 are shown in Figures 9-13.

In the LEACH protocol, the number of cluster heads is determined by comparing a random value to a threshold value. This value remains constant throughout the LEACH protocol iterations. It has been noted that in comparison to regular nodes, the cluster head loses more energy. Thus, the cluster head has a significant influence on the energy loss in LEACH. To communicate data packets to the sink node, an

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

infrastructure must be present at the very least for the cluster heads.

Although the number of cluster heads can vary depending on the threshold value, it can be challenging to reach the optimal number of nodes for a given energy level and number of live nodes.

In order to compare LEACH and AT-LEACH, we took into account 100 nodes with 5500 rounds. Figure 4 illustrates how, in the LEACH protocol, nodes begin to exhaust at the 900th round and die at the 2200th round, but in the AY-LEACH protocol, nodes begin to exhaust at the 1100th round and die at the 2400th round. In comparison to the LEACH Protocol, AT-LEACH node lifetimes are about 6% longer.

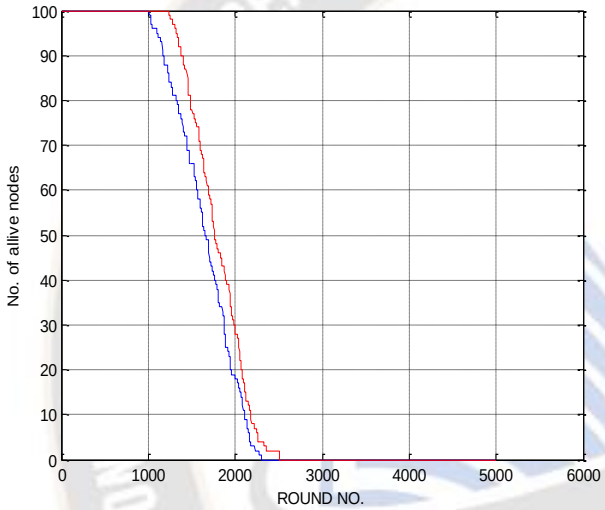

Figure 4. No. of alive nodes with the rounds

Figure 5 illustrates that in the LEACH protocol, nodes die at the 2100th round, whereas in the AD-LEACH protocol, nodes die at the 2400th round.In AT-LEACH, the Round No of Dead node is approximately 8% higher than in the LEACH Protocol.

This work allows control over the number of cluster heads by making the threshold level adaptive. By lowering the quantity of communications sent from the cluster head to the nodes, this action conserves energy.

Moreover, 08% of the total number of nodes is the upper limit on the number of cluster heads. The adaptive threshold based LEACH (AT-LEACH) protocol is the name of the protocol.

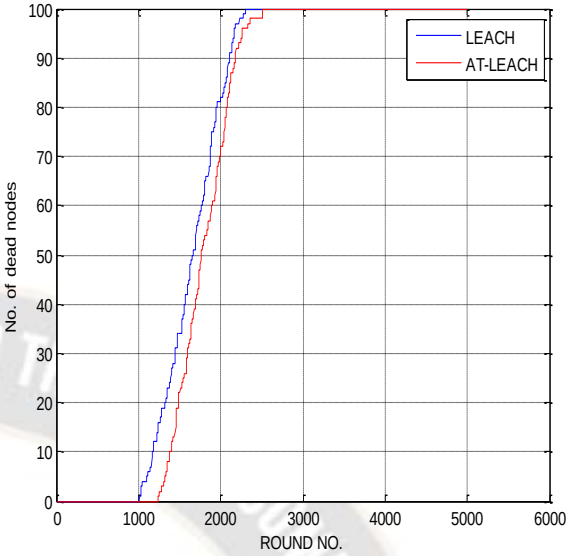

Figure 5. Dead nodes with iteration.

From the figure 6,it is seen that the Appox.11000 packets are transmitted to CHs in the LEACH protocol and In AT-LEACH the Appox.12000 packets are transmitted.

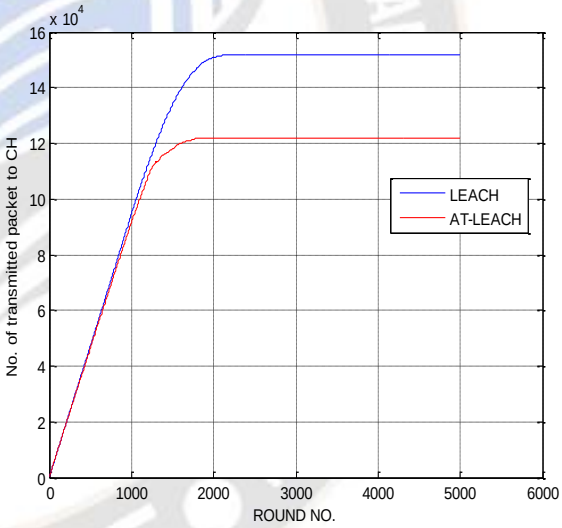

Figure 6. Round No. vs No. of Transmitted packet to CH

V. CONCLUSION

The paper concludes with a decomposition-based approach for ensuring data ordering, completion, and integrity in a generalized data transfer network. Using a distributed consensus algorithm to enforce ordering constraints, the approach divides the network into smaller sub-networks and uses distributed algorithms to verify data completion and integrity in each sub-network. The effectiveness, scalability, and robustness of the suggested approach in both simulated and real-world networks are shown by the experimental results reported in the paper. The method shows promise in

guaranteeing data ordering, completion, and integrity in distributed networks.

Subsequent research endeavors in this domain may concentrate on enhancing and refining the suggested methodology, in addition to implementing it in diverse network configurations and data transfer situations. Additionally, the suggested method can be combined with other strategies to guarantee data security and privacy in decentralized networks. All things considered, the suggested method makes a significant addition to the field of data transfer networks and is useful for a variety of applications that need safe and dependable data transfer.

References

[1] M. T. Hagan and C. H. Dagli, "Verification of data integrity, completion, and ordering in a generalized data transfer network using decomposition," IEEE Transactions on Systems, Man, and Cybernetics, vol. 24, no. 2, pp. 244-254, Feb. 1994.

[2] Fazel and M. R. Salavati, "Verification of data integrity, completion, and ordering in distributed systems," Journal of Parallel and Distributed Computing, vol. 74, no. 3, pp. 2402-2417, Mar. 2014.

[3] G. R. Guirguis and A. A. El-Sisi, "An algorithm for verifying data integrity, completion, and ordering in wireless sensor networks," Wireless Networks, vol. 17, no. 8, pp. 1923-1937, Nov. 2011.

[4] J. H. Kim and H. R. Lee, "Verification of data integrity and ordering in cloud computing systems," Journal of Supercomputing, vol. 68, no. 1, pp. 84-98, Oct. 2014.

[5] M. E. Refaat, "Verification of data integrity, completion, and ordering in peer-to-peer networks," International Journal of Computer Networks and Communications, vol. 7, no. 4, pp. 63-76, Jul. 2015.

[6] Bandchain. 2020. Band Protocol. Retrieved from https://docs.bandchain.org/whitepaper.

[7] Diana Berbecaru and Antonio Lioy. 2007. On the robustness of applications based on the SSL and TLS security protocols. In European Public Key Infrastructure Workshop. Springer, 248–264.

[8] Bitcoin.com. 2021. Bitcoin.com Co-founder Files Legal Action Against Bridge.link Token Project Over Market Manipulation. Retrieved from https://news.bitcoin.com/bitcoin-com-co-founder-files-legal-action-against-bridge- linktoken-project-over-market-manipulation/.

[9] Lorenz Breidenbach, Christian Cachin, Benedict Chan, Alex Coventry, Steve Ellis, Ari Juels, Farinaz Koushanfar, An- drew Miller, Brendan Magauran, Daniel Moroz, et al. 2021. Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. Retrieved from https://research.chain.link/whitepaper-v2.pdf.

[10] Roman Brodetski. 2017. Oracul System. Retrieved from https://gist.github.com/RomanBrodetski.

[11] Saša Milić, Burak Benligiray, and Heikki Vänttinen. 2021. API3 Decentralized APIs for Web 3.0. Retrieved from https://raw.githubusercontent.com/api3dao/api3-whitepaper/master/api3-whitepaper.pdf.

[12] Vitalik Buterin. 2014. SchellingCoin: A Minimal-Trust Universal Data Feed. Retrieved from https://blog.ethereum. org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/.

[13] Chainlink. 2021. Chainlink Achieves Major Scalability Upgrade With the Mainnet Launch of Off-Chain Reporting (OCR). Retrieved from https://blog.chain.link/off-chain-reporting-live-on-mainnet/.

[14] Corda. 2019. Corda: A Distributed Ledger. Retrieved from https://www.corda.net/content/corda-technical-whitepaper.pdf.

[15] Adán Sánchez de Pedro, Daniele Levi, and Luis Iván Cuende. 2017. Witnet: A decentralized oracle network protocol. arXiv:1711.09756. Retrieved from https://arxiv.org/abs/1711.09756.

[16] Edenchain. 2018. Edenchain. Retrieved from https://edenchain.io/wp-content/uploads/2018/08/EdenChain-Whitepaper_v1.2.pdf.

[17] S. Ellis, A. Juels, and S. Nazarov. 2017. ChainLink A Decentralized Oracle Network. Retrieved from https://link. smartcontract.com/whitepaper.

[18] Shayan Eskandari, Jeremy Clark, Vignesh Sundaresan, and Moe Adham. 2017. On the feasibility of decentralized derivatives markets. In Proceedings of the International Conference on Financial Cryptography and Data Security. Springer, 553–567.

[19] Ethereum. 2021. ERC-20 Token Standard. Retrieved from https://ethereum.org/en/developers/docs/standards/tokens/erc-20/.

[20] IOTA Foundation. 2021. Introducing IOTA Oracles. Retrieved from https://blog.iota.org/introducing-iota-oracles/.

[21] Vahid Garousi, Michael Felderer, and Mika V. Mäntylä. 2019. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf. Softw. Technol. 106 (2019), 101–121.

[22] Gnosis. 2017. Gnosis. Retrieved from https://github.com/gnosis/research/blob/master/gnosis-whitepaper.pdf.

[23] Juan Guarnizo and Pawel Szalachowski. 2019. PDFS: Practical data feed service for smart contracts. In European Symposium on Research in Computer Security. Springer, 767–789.

[24] J. He, R. Wang, W. Tsai, and E. Deng. 2019. SDFS: A scalable data feed service for smart contracts. In Proceedings of the IEEE 10th International Conference on Software Engineering and Service Science (ICSESS'19). IEEE, 581–585.

[25] Jonathan Heiss, Jacob Eberhardt, and Stefan Tai. 2019. From oracles to trustworthy data on-chaining systems. In

[26] Hrishikesh Huilgolka. 2019. Razor Network: A Decentralized Oracle Platform. Retrieved from https://razor.network/ whitepaper.pdf.

[27] Hyperledger. 2014. Hyperledger Fabric. Retrieved from https://hyperledger-fabric.readthedocs.io/.

[28] JustLink. 2020. BJustLink A Decentralised Oracle Network on TRON. Retrieved from https://docs.justlink.io/ whitepaper/justlink_whitepaper_v1.0.pdf.

[29] Protocol Labs. 2021. InterPlanetary File System (IPFS). Retrieved from https://docs.ipfs.io/.

[30] Ledger. 2020. Ledger Troubleshooting. Retrieved from https://support.ledger.com/hc/en-us.

[31] Guozhu Liang, Wei Wu, and Jingyu Wang. 2021. Polkaoracel A Substrate-based Self-evolving Oracle System. Re- trieved from https://polkaoracle-1.gitbook.io/polkaoracle-wiki/.

[32] Wenzhu liang. 2021. Polkadot-based Decentralized Cross-chain Prediction Platform. Retrieved from https://x-predict. com/X_Predict_market_Whitepaper_en.pdf?v=1.0.

[33] Mhamane Sanjeev Chandrashekhar,1 Amol Kumbhare2* "The Integrated SDL-based design approach to create and implement wireless communication protocol" Journal of Integrated Science and Technology, (2023).