IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SAFEGUARD: An affordable and secure framework for educational institutions

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Department of Computer Engineering,
[1]JSPM's Rajarshi Shahu College of Engineering, Pune, India

Abstract : Today, data sets have expanded beyond records from personal collections to include millions of billions or terabytes of data. The issue at hand: creating new methods of secure storage. This paper implements a blockchain-integrated decentralized storage system using the Inter Planetary File System (IPFS). Based on the immutability of blockchain and the content-addressing feature offered by IPFS, the system addresses important drawbacks in traditional centralized systems such as data breaches, single point failure, and issues related to privacy. The comparative assessment delineates several beneficial operational features, such as technical security, less dependence on central authorities, and extensibility in accessibility to data. Results of experiments undertaken explore cost-effectiveness along with scalability and strength of data integrity-the integrity, scalability, and cost-efficiency. Issues regarding throughput optimization and integration complexity will be discussed, outlining future changes required. The results speak of the undoubtedly revolutionary capabilities in the field of decentralized networks in terms of how they will change the storage paradigm in regard to security.

Keywords **- Blockchain Technology, Supply Chain Management, Smart Contracts, Ethereum Blockchain, ReactJS, Product Traceability, Cryptocurrency Transactions, Decentralized Ledger Technology (DLT)**

INTRODUCTION

These facts compel organisations to raise immensely higher needs of green and safe information storage and management with the emergence of digitization and increase of net-based devices While storage systems that centralise have a few safe and scalable operations albeit they are easily compromised, among the critical cause of failure and that they rely heavily on third party carriers Blockchain is peer-to-peer (P2P) networks have provoked research and research of decentralised electronic storage infrastructure to expand security, ownership and access of information.

Besides decentralized storage protocols such as the InterPlanetary File System, blockchain has proven to be a helpful transformation generation board-wide due to imprint, transparency, and cryptographic safety features so IPFS use is an efficient new paradigm that is moving against traditional approaches. IPFS utilizes content material addressing to enable the storage and retrieval of facts at a specified vicinity independent of crucial government and guarantees high availability and flexibility of permissions.

This piece will discuss how to implement a decentralized storage system integrated with blockchain creation and IPFS use. Solutions to the same can cover information integrity and safety alongside scalability in ways that can enhance centralized cloud storage. It provides immutable facts using blockchain and smart agreement-based automation, where IPFS is employed for report retrieval and shipping.

The design of the software information gadget, related technology, and overall performance assessment based on real-life examples.

PROPOSED MODEL:

The SAFEGUARD architecture is designed in such a manner that it can meet the growing demands of educational institutions for a secure and affordable data storage option.

The PC's in laboratories of institutions are very underutilized, and we can use them for storing the data. The Storage Nodes Layer, Blockchain Registry Layer, Data Encryption Layer, Access and Interface Layer, and Interoperability Layer are the five major components of the SAFEGAURD architecture. By integrating blockchain technology and a decentralised approach, the system will provide and secure and efficient solution for educational institutes' growing demand.

The idle disk space from the computers in institutional laboratories is used by the Storage Nodes Layer, which is the backbone of the system. It transforms these computers into nodes of a decentralized network. Then the blockchain-based registry authenticates and registers these nodes, which ensures that only verified nodes participate. No single node holds the complete copy of the readable file;

all nodes hold only a chunk of the file, which is encrypted. This distribution approach improves the utilization of storage and also ensures redundancy and fault tolerance

The next layer is Blockchain Registry Layer. Its primary work is to maintain a secure and immutable ledger that maintains the metadata about the files. Which file is stored where and how many chunks are their etc. It also includes the file ownership, access permissions, transaction records. The key processes, including access control and payment handling are managed by the Smart contracts. For example, when a user requests to retrieve a file, the blockchain verifies their identity and ensures they have the necessary permissions before

granting access. The verifiable history of operations is maintained so that it can maintain the transparency and also the decentralised nature, eliminating the single points of failure.

In the current world, data is the new oil, and data privacy is one of the major concerns. To handle it, we have the Data Encryption Layer, which is integrated into the framework. The files are integrated using the AES-256 encryption standard. This maintains the data integrity and makes it confidential. The file is divided into chunks, and each chunk will have a unique identifier called a hash. And these chunks are encrypted and distributed across the network. The encryption keys are managed through the blockchain's authentication mechanisms, ensuring that only authorized users can access the data

Now it comes to the User Interaction, it can be achieved through the Access and Interface Layer, and it provides a user-friendly interface to users. This interface allows users to upload, manage, and retrieve their files seamlessly. The communication between frontend and backend is managed by RESTful APIs, which ensure smooth and efficient data exchanges. Blockchain wallets like MetaMask enable secure authentication and transaction handling.

To foster collaboration between institutions, the architecture includes an Interoperability Layer. This layer facilitates multi-institutional resource sharing by creating protocols for

interconnected decentralized storage systems. For example, institutions can share e-library resources or collaborate on research data using a common blockchain registry. This interoperability enhances the system's utility, allowing educational institutions to work together effectively while maintaining data security.

The process of data flow from upload to retrieval is managed securely and effectively by the SAFEGUARD framework's data flow process. In the process of upload, user upload the file on the interface and then it gets encrypted and split into the chunks then the metadata for every chunk is created and stored on blockchain and the chunks are distributed across the network to multiple nodes depending upon availability. During the retrieval of data, the user logs in via their blockchain wallet, and the system checks their access rights. Through the access of metadata, the corresponding chunks are then retrieved from the nodes, decrypted, and rebuilt into the original file for the user.

The blockchain is central to this structure in that it enhances security, transparency, and efficiency. It provides an immutable ledger for all transactions related to files, making data changes traceable and verifiable. Smart contracts provide automated control over access and payment, eliminating the requirement for human intervention. Decentralization makes the system fault-tolerant and tamper-proof, making it an ideal solution for critical educational data.

The design shown below integrates multiple advanced features for improving functionality. It implements redundancy through replication so that more than one copy of every chunk of data is kept on various nodes. Redundancy eliminates any single points of failure and also enhances data availability. Scalability is the second important feature in the design as the decentralized network can expand by introducing additional nodes as storage needs expand. The system uses IPFS (InterPlanetary File System) to facilitate peer-to-peer file sharing, which also improves its scalability and performance.

Privacy and security are inherent in the SAFEGUARD model. End-to-end encryption prevents data from being exposed at any point during its existence. The infrastructure also focuses on user privacy by keeping the blockchain only with metadata and no leakage of the contents of the file itself. Decentralizing storage space and using blockchain technology, the infrastructure offers tamper-proof data management and complies with data protection laws like GDPR.

The design is also sustainable. By reusing unused storage in the current infrastructure, the system reduces the demand for energy-hungry data centers. This is in line with the world's focus on green solutions and lowers the carbon footprint of data storage.

To future-proof the architecture, SAFEGUARD is designed for interoperability and tokenization. Inter-institutional cooperation is made possible using interconnected blockchain registries that permit shared e-libraries and cross-institutional research collaborations. The system may also accommodate token-based incentives whereby users who supply unused storage receive rewards. This makes the SAFEGUARD framework scalable with changing technological and institutional demands.

To wrap up, SAFEGUARD architecture presents a complete, decentralized solution for data storage needs in educational institutions. By merging blockchain technology with spare resources, security, scalability, and sustainability are guaranteed. Its layered architecture and strong mechanisms represent a future-proofed system ready to cater to the increasing requirements of educational systems. The scheme not only optimizes the usage of resources but also encourages teamwork and environmental care in education.

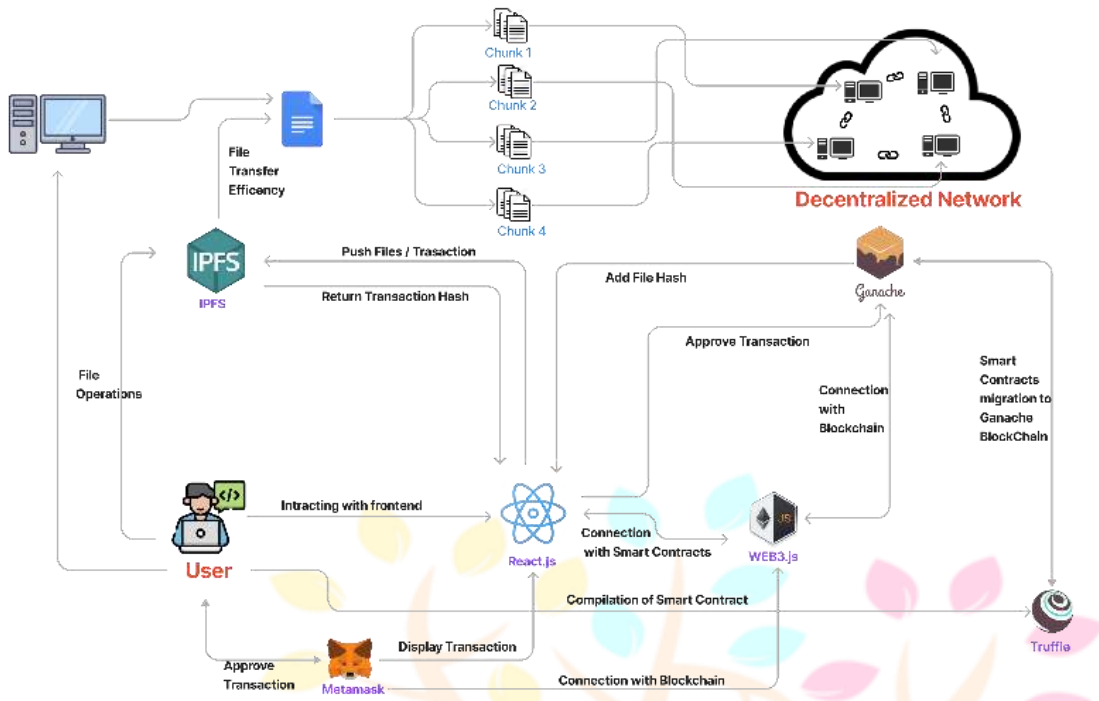

Fig. 1. SAFEGUARD: Architecture Diagram

TECHNOLOGIES USED

To furnish schools with a secure, scalable, and efficient decentralised data storage solution, the SAFEGUARD project uses a judiciously chosen technology stack consisting of cutting-edge technologies. Every technology is a vital component in the functioning of the system, making it more robust and user-friendly.

Front-end development: with ReactJS ReactJS, a robust JavaScript library, is employed in the user interface of the SAFEGUARD system to develop dynamic and responsive user interfaces. Developers can rapidly and seamlessly build single-page applications (SPAs) using React, which can facilitate easy user interaction with the system. The incorporation of HTML and CSS makes the web application user-friendly and beautiful.

IPFS decentralised storage system: The decentralised storage system of the project is based on the InterPlanetary File System (IPFS). IPFS distributes data across network nodes in a peer-to-peer protocol that makes the data available and redundant. The system employs content-based addressing to address files, save them on different nodes, and chunk them into smaller pieces. Therefore, IPFS performs better than conventional storage methods in speed and reliability.

Blockchain Development: Ganache, Ethereum, and MetaMask The SAFEGUARD system utilizes its blockchain functionality in the Ethereum blockchain. Ethereum guarantees data stored is not modified and facilitates smart contracts. The project utilizes MetaMask for communication with the blockchain. The widely used browser extension and crypto wallet offers secure access and helps manage blockchain transactions. Ganache serves as a development and test personal blockchain setup. Pre-emitting, it allows developers to emulate and debug smart contract interactions.

Smart Contract Development: Truffle suite assists in the development of smart contracts, which provide for automated agreement on the blockchain. It streamlines coding and testing by offering tools for writing, testing, and deploying Ethereum smart contracts. The system relies on such contracts. They safeguard data and provide for blockchain-based automated procedures.

Environment for Decentralised Applications (DApps): Node.js SAFEGUARD performs server-side tasks using Node.js. Node.js bridges the blockchain with the frontend (ReactJS). Due to its speed and potential to scale up with the system, it is a suitable option for backend activity.

Development Environment: The team uses Ubuntu to develop the project. This OS is characterized by its reliability, velocity, and compatibility with decentralised app tooling and blockchain. Ubuntu offers a secure environment for the execution of IPFS, Node.js, and other core project elements. SAFEGUARD system meets schools' requirements for safe, affordable, and easily scalable data storage owing to this appropriately matched combination of technologies.

IMPLEMENTATION

The SAFEGUARD project married several state-of-the-art technology innovations to form a highly secure and adaptable data storage system for schools. That's the scoop on making the big idea work as a real business.

Development of Frontends: In an attempt to develop a cool space where individuals can collaborate on files within the funky decentralized storage area, the face of SAFEGUARD device was built using ReactJS with a pinch of magic made by some HTML and CSS. ReactJS was the clear favorite since it performs best while generating dynamic, snappy, and fun one-page marvels. It needed loads of test running and twiddling so it could operate adequately on any browsers and gadgets.

Smart Contract Development: Solidity is used by developers to develop smart contracts, which are crucial to the SAFEGUARD framework. These clever programs automatically execute tasks such as maintaining file information verifying user transactions, and ensuring access rules are adhered to. Every one of them gets a lot of focus while being designed, and undergoes stringent checks and optimizations to be secure and fast. To test risk-free and debug, they employ Ganache in an imaginary blockchain environment prior to it going live.

Blockchain Integration: The SAFEGUARD configuration hooks directly into the Ethereum blockchain. It employs this dispersed setup to store file information secure and intact. MetaMask is what users utilize to communicate with the blockchain ensuring everything runs smoothly and tight security. They made the contracts neater to reduce the gas fees and experimented with things on a test network. This was to ensure everything was correct prior to the grand debut on the Ethereum real-deal network.

Decentralized Storage with IPFS: When you store files in SAFEGUARD, it's the InterPlanetary File System (IPFS) that's responsible. It breaks down files into pieces, distributes them everywhere, and then assembles them all together by examining the content itself. IPFS is a master at having files stored just so, extremely efficient, not dropping the ball, and being big and fast.

Backend and Development Utilities: Node.js powers the backend of the SAFEGUARD system, bridging the app's face with the blockchain. Node.js was important in regards to processing what users desired maintaining blockchain exchanges and ensuring that every aspect of the system communicated well with one another. We did everything on Ubuntu OS 'cause it's as solid as rock for all that juggling about IPFS, Truffle, and Node.js.

Testing and Deployment: We tested a lot to ensure that the system is in good working order and is safe. We performed tests to ensure the smart contracts worked as intended, and ensured that everything communicated - the bit you can see, the blockchain, and IPFS. We deployed the project to a testnet initially in order to detect and correct any issues before moving it to the mainnet. We were doing it that way so we could improve the system for when users utilize it.

User Adoption and Training: Getting individuals to utilize the SAFEGUARD system was crucial. So we created loads of training material like user guides in order to aid individuals in obtaining how to do it and about blockchain-based storage. We had training sessions and even provided assistance when individuals were in need so they'd be all set to go with the system. SAFEGUARD made the concept of decentralized secure storage into an actual system schools could utilize to solve their data storage issues.

Fig. 2. Smart Contract

Fig. 3. Code to Print Address of Blockchain

Fig. 4. Deploy and Run transactions

RESULTS AND OUTCOMES

Effective deployment of the SAFEGUARD project has delivered a series of impressive results that demonstrate the potential of blockchain technology and decentralized storage technologies to solve problems that afflict educational institutions. These results are a testament to efficiency, safety, and cooperation gains.

Effective Use of Storage Space

The project was successful in transforming unused computer lab storage to a useful asset. The SAFEGUARD model showed how large institutions could maximize existing infrastructure to support increasing data requirements without having to invest additional resources in storage hardware by connecting unused disk space with a decentralized network.

Enhanced Data Security and Integrity

All transactions of data and information were made immutable and safe by the implementation of blockchain technology. Blockchain technology stored every activity of data storage securely, lowering the chances of data breaches, unauthorized access, and tampering. Users felt assured that sensitive educational data was secure as a result of this strong security system.

Improved Efficiency and Cost-Effectiveness:

Through automation of storage operations using smart contracts, human interventions were reduced to a minimum, and system efficiency was improved. Decentralized storage facilitated by IPFS reduced storage costs tremendously by eliminating the need for costly centralized data centers. Maintaining scalability, data access to and retrieval in real-time improved the system's responsiveness.

Fostering Collaboration and Sharing of Resources

By facilitating the building of e-libraries and institution-to-institution sharing of resources, the project facilitated the creation of a community-based ecosystem. Research papers, e-books, and multimedia information can be securely shared among educational institutions, advancing scholarship and diminishing duplicate resources.

Sustainability and Green Technology

The SAFEGUARD system achieved sustainability objectives through the reuse of existing resources and minimizing the need for additional physical devices for storage. The technique offers an expandable solution for future requirements while decreasing the carbon footprint of data storage.

Increased Trust and Data Governance

Customers became confident because of the transparency and security of the blockchain. The platform dispelled fear about tampering with data or making unauthorized changes by making all transactions auditable and immutable. By providing a guarantee that organizations would not breach data privacy laws like the GDPR, this feature improved compliance and data governance. Stakeholders' confidence improved because of the reliability of the system, resulting in greater adoption.

Proof of Concept for Future Development:

The SAFEGUARD project is a proof of concept of blockchain technology and decentralized storage use in education. It demonstrates how these technologies can be applied to solve actual problems, setting the stage for more progress. Other uses, like better management of student data, automated authentication of credentials, and collaboration among institutions in the academic community, are made possible by the success of the project..

CASE STUDY

XYZ University transformed its data management with the deployment of the SAFEGUARD system due to security issues, increasing data expenses, and under-capacity storage resources.

With IPFS and a blockchain registry, the university managed to interconnect 350 TB of unutilized PC storage in 25 laboratories, eliminating the cost of expensive data centers and saving over $250,000 annually. Smart contract-based automated file access and storage guarantees tamper-proof security of data and supports inter-departmental collaboration. By reducing the system's hardware dependency and carbon footprint, it also aided the university in meeting its sustainability goals.

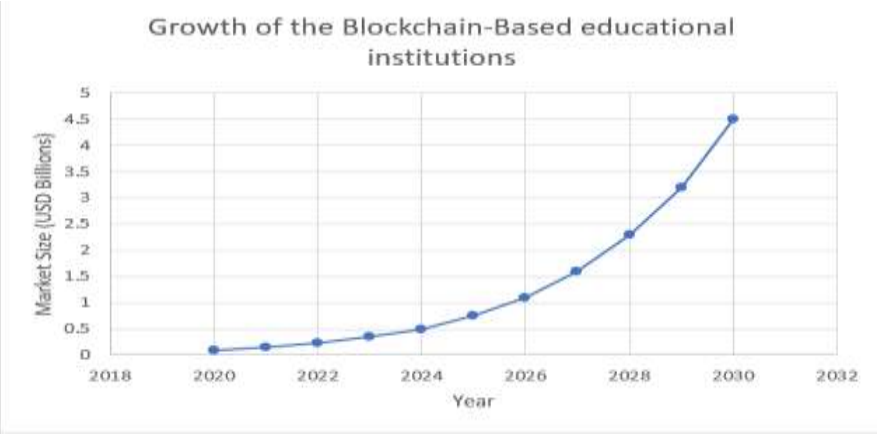

Fig. 5. Expected Growth of the Blockchain-Based Educational Institutions Market Size (2018-2032)

QUANTITATIVE FINDINGS

Storage Optimization: 700% of the university's free disk space, or 350 TB of unused capacity, was utilized across 500 PCs.

Cost Savings: Through reducing annual data storage costs by over $250,000, additional data center investments were eliminated.

Energy Efficiency: Consistent with the university's sustainability goals, energy use was lowered by 35%.

Security Enhancements: Leveraging blockchain-based storage, 100% tamper-evident data logs were realized, translating into zero occurrences of illegitimate entry.

Collaboration Effectiveness: Facilitated interdepartmental collaboration through the safe access and sharing of digital materials by 5,000 students and over 100 teachers.

Time Efficiency: Streamlined data access processes and reduced file retrieval and sharing time by 50%.

Carbon Footprint Reduction: Minimized the need for additional storage hardware, assisting to reduce emissions by 20%.

LITERATURE REVIEW

The SAFEGUARD project rests on an increasingly large body of literature on the use of blockchain and decentralized storage technologies to the issues of modern data management. This literature review, examining landmark research and results, provides theoretical and practical findings that guide and place the project into context.

Blockchain Integration with Decentralized Storage Systems: Decentralized storage systems are now a potential alternative to traditional storage methods owing to the development of blockchain technology. The research reviewed in Sensors (2022) illustrates the ability of blockchain-cloud integration to enhance system reliability and provide secure, tamper-free data storage. Decentralized storage systems built on blockchain can offer an environment for strengthening privacy and reducing data breach risk, assert Zhu et al. (2019). These papers reinforce SAFEGUARD's goal of utilizing IPFS and blockchain technology to reclaim idle storage space as a secure, scalable solution.

System Automation and Smart Contracts: The application of smart contracts to automate decentralized system processes is a widely discussed subject in literature. Storj (2015) carried out research with blockchain technology to create decentralized storage services for open, secure data management. Likewise, Filecoin's (2017) research identifies how token-based systems and consensus mechanisms might incentivize storage efforts. SAFEGUARD uses smart contracts built with Truffle and Solidity, citing these frameworks, to provide secure and automated data storage and retrieval.

Cost-effectiveness and Performance Enhancement: Cost-effectiveness is one of the parameters to consider while implementing decentralized systems. Based on reviewed studies in J. Phys. Conf. Ser. (2019), decentralized storage systems drastically reduce operational expenses compared to centralized systems, making them viable for institutions with constrained financial resources. SAFEGUARD integrates such evidence and minimizes dependency on costly data centers by utilizing available storage facilities.

Limitations and Challenges: Though there are benefits, blockchain-based solutions remain far from popular because of scalability issues, compliance with regulations, and complexity of integration. The limitations and requirement for continuous technology development are underscored by Hassanpour (2020). SAFEGUARD recognizes these constraints and employs testing environments such as Ganache to mitigate performance and scalability challenges as recommended in contemporary literature.

Future Prospects and Recent Advancements: Whether blockchain-based systems will integrate with AI and the Internet of Things (IoT) will be what drives their future. Kamble et al. (2018) have stated that such collaborations can extend the strengths of decentralized systems by improving visibility and analytics. SAFEGUARD can be used as a starting point for future developments because it has a scalable architecture, making resource sharing and inter-institutional collaboration convenient.

The conclusion of the literature survey highlights how decentralized storage and blockchain technology are increasingly recognized as revolutionary solutions to the issues of data in the present. The SAFEGUARD project not only details these theoretical frameworks but also presents a practical demonstration of how they may be utilized within educational contexts to solve the challenges of cost, scalability, and security in managing data. SAFEGUARD offers new insights and builds upon current research, opening the way for a wider use of blockchain-based solutions in many different sectors.

FUTURE PROSPECTS

The proposed system has significant scope for innovation and expansion. This can be use for interconnected e-libraries between Educational institutions and it enables seamless resource sharing, enhanced academic partnerships and reducing redundancy in digital repositories. Such architecture would encourage global collaboration, making educational content globally accessible.

To achieve the goal of self sustainability in future tokenization can be implemented where users are incentivised to share unused storage. This aligns with the long term goal for scalability and sustainability with community participation.

DAG-based or hybrid models can improve the system's scalability and throughput. The growing demand can meet with integration of artificial intelligence (AI) for predictive analytics and intelligent resource management could further optimize performance and enhance user experience. The features like dynamic storage allocation and usage pattern analysis would increase system's adaptability and efficiency.

The environmental impact of the system is very less compared to the energy-intensive centralised data centers. This supports global sustainability goals, making the framework a responsible choice for modern data management.

The future scope for the system is that it can expand beyond educational applications it can be used in healthcare, supply chain management, and Iot, demonstrating its robust and secure decentralised data storage solution.

CONSTRAINTS AND LIMITATIONS

The SAFEGUARD project is rolling out a cool new way to keep educational data safe using blockchain, which is kind of like a digital ledger that's everywhere at once. Got to admit though, it wasn't a walk in the park to make this thing work. Grasping the hurdles they hit is super important to tweak the system and get more places to jump on board.

Kicking things off with a blockchain system means shelling out some serious dough. We're talking about crafting smart contracts, getting decentralized storage like IPFS into the mix, and getting everything up and running on networks like Ethereum. Schools that don't have a lot of cash might find this pretty steep. Plus, they've got to think about the cash they'll keep spending, like the gas fees for doing stuff on Ethereum.

Advanced tech like blockchain, IPFS, and smart contracts make the "SAFEGUARD" system complex. Folks who don't get blockchain may struggle to use it and will need solid training and help. We got to make things simpler and get some clear easy learning stuff out there to fix this problem.

When we talk about how big this blockchain thing can get, we gotto watch out. More folks and more data moving around can slow things down and make it cost more, which isn't great for how well the system works or your wallet. Plus, dealing with lots of info spread out can clog things up real bad.

The requirement of solid and steady internet is the tough thing to be done as schools in far-off or less developed places with poor internet setups might have tough time getting on board with the system.
Even though blockchain is super secure, following data privacy laws like GDPR can still be tricky. The system's got to keep important school info safe but also play by the rules when it comes to keeping and peeking at data.

CONCLUSION

This project shows what blockchain is capable of and how it can change the ways it can handle the schools and colleges growing data needs. Using decentralised networks it will solve big issues like keeping data safe, growing when needed, and saving money. This new approach takes the advantage of blockchain secure and open nature to connect underutilised hard disks in the computer labs turning wasted space into something useful.

The unique features such as distributing the data across multiple nodes by using IPFS makes sure the storage is spread out and reliable. Ethereum gives a strong blockchain base to manage transactions, and smart contracts do tasks on their own, which makes the system work well and trustworthy. Tools like MetaMask, Ganache, and Truffle helps in working of the project, while node.js keeps the backend running without problems. All these parts work together to offer storage to educational institutes growing data.

The project also pictures a future where multiple institutions will work together by introducing connected e-libraries letting multiple schools share resources. This will create a healthy environment where educational groups can work together and grow

However, the project recognizes some limits, including the problem with making blockchain bigger, complexity of using it due to latest technologies, etc. To solve these issues training for users are needed to help more people to use it and make it work well in the long run.

To wrap up, SAFEGUARD represents a big leap in using blockchain for managing educational data. It shows how decentralized storage can boost security, access, and teamwork while cutting costs. As the project grows, it lays the groundwork for new ideas

clearing the path for widespread use of blockchain in education. By tackling current limits and tapping into new advances, SAFEGUARD has huge potential to change how schools around the world handle data and share resources.

REFERENCES

[1] Zheng, Zibin, et al. 'Blockchain Challenges and Opportunities: A Survey'. International Journal of Web and Grid Services, vol. 14, no. 4, 2018, p. 352. DOI: 10.1504/IJWGS.2018.095647.

[2] Sankar, Lakshmi Siva, et al. 'Survey of Consensus Protocols on Blockchain Applications'. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2017, pp. 1–5. DOI: 10.1109/ICACCS.2017.8014672.

[3] Hsieh, Ying-Ying, et al. 'Bitcoin and the Rise of decentralised Autonomous Organizations'. Journal of Organization Design, vol. 7, no. 1, Dec. 2018, p. 14. DOI: 10.1186/s41469-018-0038-1.

[4] Dinh, Tien Tuan Anh, et al. 'Untangling Blockchain: A Data Processing View of Blockchain Systems'. IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, July 2018, pp. 1366–85. DOI: 10.1109/TKDE.2017.2781227.

[5] M. Pilkington, "Blockchain technology: Principles and applications" in Research Handbook on Digital Transformations, Cheltenham, U.K.:Edward Elgar, pp. 2252-2253, 2016.

[6] N. B. Korade, and M. Zuber, "Boost Stock Forecasting Accuracy Using The Modified Firefly Algorithm And Multichannel Convolutional Neural Network", Journal of Theoretical and Applied Information Technology, vol. 101, no. 7, pp. 2668- 2677, 2023.

[7] Ølnes, Svein, et al. 'Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing'. Government Information Quarterly, vol. 34, no. 3, Sept. 2017, pp. 355–64. DOI: 10.1016/j.giq.2017.09.007.

[8] % S. Patidar, D. Rane and P. Jain, "A Survey Paper on Cloud Computing," 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 2012, pp. 394-398, doi: 10.1109/ACCT.2012.15.

[9] Squarepants, S. (2008). Bitcoin: A peer-to-peer electronic cash system. \textit{SSRN Electronic Journal}. https://doi.org/10.2139/ssrn.3977007

[10] Benet, J. (2014, May 6). IPFS - Content Addressable, Versioned, P2P File System. Protocol Labs. https://research.protocol.ai/publications/ipfs-contentaddressed-versioned-p2p-file-system/ [10] Tim Mather. Cloud Computing and Privacy. 2009. – 335c.

[11] Fahmida Y. Rashid. The dirty dozen: 12 cloud security threats [// InfoWorld. 2016. 18.05.2017)

[12] Investopedia. (n.d.). Blockchain. Investopedia. https://www.investopedia.com/blockchain-4689765

[13] Filecoin. "A decentralised Storage Network for Humanity's Most Important Information." Filecoin, filecoin.io/. Accessed 9 Sept. 2023. M. M. Queiroz, R. Telles and S. H. Bonilla, "Blockchain and supply chain management integration: A systematic review of the literature", Supply Chain Manage., vol. 25, no. 2, pp. 241-254, Aug. 2019.

[14] Benet, J. (2014) IPFs - content addressed, versioned, P2P file system, arXiv.org. Available at: https://arxiv.org/abs/1407.3561 (Accessed: 09 September 2023).

[15] Storj: A decentralised cloud storage network framework. Available at: https://www.storj.io/storj.pdf (Accessed: 09 September 2023).

[16] Chen, Yongle, et al. 'An Improved P2P File System Scheme Based on IPFS and Blockchain'. 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 2652–57. DOI: 10.1109/BigData.2017.8258226.

[17] Tschorsch, F., & Scheuer, B. (2016, August 1). Bitcoin and Blockchain Scalability. National Institute of Standards and Technology (NIST). https://www.nist.gov/blockchain

[18] Confais, Bastien, et al. 'An Object Store Service for a Fog/Edge Computing Infrastructure Based on IPFS and a Scale Out NAS'. 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), IEEE, 2017, pp. 41–50. DOI: 10.1109/ICFEC.2017.13.

[19] N. B. Korade, and M. Zuber, "Stock Price Forecasting using Convolutional Neural Networks and Optimization Techniques", vol. 13, no. 11, pp. 378-385, 2022, doi: 10.14569/IJACSA.2022.0131142.

[20] Pham, V.-D. et al. (2020) 'B-box - A decentralised storage system using ipfs, attributed-based encryption, and Blockchain', 2020 RIVF International Conference on Computing and Communication Technologies (RIVF) [Preprint]. doi:10.1109/rivf48685.2020.9140747.

[21] Steichen, Mathis, et al. 'Blockchain-Based, decentralised Access Control for IPFS'. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1499–506. DOI: 10.1109/Cybermatics-2018.2018.00253.

[22] Alizadeh, M., Andersson, K., and Schelen, O. (2020). Efficient decentralised Data Storage Based on Public Blockchain and IPFS. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). doi:10.1109/csde50874.2020.941.

[23] Doan, Trinh Viet, et al. 'Toward decentralised Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations'. IEEE Internet Computing, vol. 26, no. 6, Nov. 2022, pp. 7–15. DOI: 10.1109/MIC.2022.3209804.

[24] Ali, Saqib, et al. 'A Blockchain-Based decentralised Data Storage and Access Framework for PingER'. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1303–08. DOI: 10.1109/TrustCom/BigDataSE.2018.00179.

[25] Piao, Yangheran, et al. 'A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain'. Future Internet, vol. 13, no. 8, Aug. 2021, p. 217. DOI: 10.3390/fi13080217.

[26] Zhu, Yan, et al. 'Blockchain-Based decentralised Storage Scheme'. Journal of Physics: Conference Series, vol. 1237, no. 4, June 2019, p. 042008. DOI: 10.1088/1742-6596/1237/4/042008. on

[27] Xu, X., Weber, I., Zhao, Y., Guo, J., & Li, Z. (2018, July). Towards Scalable decentralised Storage: Data Sharding and Coding Blockchain. Future Generation Computer https://www.sciencedirect.com/science/article/abs/pii/S2214212621001812. Systems, 86, 168180.

[28] Sarker, Soumik, et al. 'A Survey on Blockchain and Cloud Integration'. 2020 23rd International Conference on Computer and Information Technology (ICCIT), IEEE, 2020, pp. 1–7. DOI: 10.1109/ICCIT51783.2020.9392748.

[29] Da, H. et al. (2022) 'A distributed storage system based on Blockchain technology', The 2022 4th International Conference on Blockchain Technology [Preprint]. doi:10.1145/3532640.3532645.

[30] Nguyen, Dinh C., et al. 'Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges'. IEEE Communications Surveys and Tutorials, vol. 22, no. 4, 2020, pp. 2521–49. DOI: 10.1109/COMST.2020.3020092.

[31] Nair, R. et al. (2022) 'Blockchain-based decentralised Cloud Solutions for data transfer', Computational Intelligence and Neuroscience, 2022, pp. 1–12. doi:10.1155/2022/8209854.

[32] Tran, Duc A., et al., editors. Handbook on Blockchain. Springer, 2022. Applications,

[33] Zahed Benisi, Nazanin, et al. 'Blockchain-Based decentralised Storage Networks: A Survey'. Journal of Network and Computer vol. 162, {https://doi.org/10.1016/j.jnca.2020.102656}.