Grenze International Journal of Engineering and Technology, January Issue

Decentralized File Sharing System on Solana Blockchain: Bridging Web 2.0 and Web 3.0

Thejaswini S[1], Chandana[2] and Chinmayi B[3]
[1]Assistant Professor, Department of CSE, Siddaganga Institute of Technology, Tumkuru, Karnataka India
Email: thejaswinis@sit.ac.in
[2-3]UG Students, Department of CSE, Siddaganga Institute of Technology, Tumkuru, Karnataka India
Email: chandana3702@gmail.com, chinmayibasavaraju13@gmail.com

***Abstract*—In the present digitized era, the exploration of web3 is bringing revolution in the internet by advocating the importance for user centric decentralized platforms with enhanced security. Hence, the paper looks into the advancements of the World Wide Web over the years and introduces highlights on Solana Blockchain along with one of its applications namely decentralized file sharing system. Centralized file sharing systems are vulnerable to censorship and corruption. When a single entity controls the system, it becomes easy for governments or other concerned organizations to block or manipulate access control and data on the files of any user. To overcome this issue, a decentralized file sharing system leveraging Solana blockchain and Interplanetary File System(IPFS) is proposed in the paper. In this proposed work, Solana file storage and retrieval is facilitated by IPFS, which ensures the transparency and flexibility of decentralized file sharing operations over the network by reducing the reliance on centralized servers. Therefore, the usage of the integrated platforms in the proposed work enhances the system performance w.r.t transaction speed, transaction cost and security.**

***Index Terms*— Blockchain, Solana, Interplanetary File System, Web 3.0.**

I. INTRODUCTION

The internet has encountered various changes over the years, from the static web of Web 1.0 to the dynamic and interactive platforms of Web 2.0, and now towards the decentralized paradigm of Web 3.0. Web 1.0 was characterized by static web pages with limited interactivity and centralized content creation, laying the groundwork for the modern internet. With the emergence of Web 2.0, there was a shift towards user-generated content, social networking, and richer user experiences, marking a significant departure from the one-way communication model of Web 1.0.

Web 3.0 represents the next stage in the internet's evolution, emphasizing decentralization, interoperability, and user control. At the core of Web 3.0 is blockchain technology, which enables secure, transparent, and decentralized digital transactions. Blockchain serves as a distributed ledger it records transactions across a network of computers in a tamper-evident and immutable manner, providing a foundation for trustless and censorship-resistant systems.As per our survey knowledge, there are not many papers which address web 3.0and its applications. So,in this paper, the focus is on solana blockchain. Solana blockchain is one of the open source, efficient, fast and cost less blockchains.Many applications are developed and are being developed using Solana. One such application is the decentralized file sharing system on solana blockchain which is focused in the proposed work.

Grenze ID: 01.GIJET.11.1.544_1

In this context, decentralized file sharing systems have garnered attention as alternatives to traditional centralized platforms. Centralized systems are vulnerable to censorship and corruption, as a single entity controls access to files. This poses serious risks to both organizations and individuals that rely on these systems for sharing sensitive or important information. To solve these challenges, decentralized file sharing systems leverage blockchain technology and peer-to-peer networks to create distributed and secure platforms for file storage and sharing.

This paper covers the integration of Solana blockchain and the InterPlanetary File System (IPFS) to develop a decentralized file sharing system. By leveraging Solana's high-performance blockchain and IPFS's decentralized file storage capabilities, the proposed work aims to overcome the restrictions of centralized platforms while ensuring transparency, security, and scalability in file sharing operations. The paper outlines the architecture, implementation, and future directions of the system, demonstrating its potential to foster a more resilient and accessible file sharing ecosystem in the era of Web 3.0.

A. Related Work

Blockchains are ineffectual for distributing and storing large data, according to the study in [1]. Users can swiftly share large files while still benefiting from the blockchain. Cryptographic hashes can be provided to the latter, proving that the file was available to someone at a specific time. The Interplanetary File System (IPFS), which combines file sharing and the aforementioned hashes, is a particularly attractive file sharing platform for this purpose. IPFS identifies, verifies, and transports files on the basis of their cryptographic hashes. Similar to public blockchains, files stored on IPFS can be read and viewed by anybody who can connect to or build an IPFS node. For blockchain apps that interface with large files holding sensitive or personal information, this is a concern. As a result, this paper builds an IPFS with access control using the Solana blockchain. A Solana smart contract stores and dynamically modifies the access control list. The modified IPFS software, termed ACL-IPFS in the following, can then connect to the smart contract and enforce the access control list's rights. ACL- IPFS allows users to register new files and give and withdraw permissions by producing and submitting transactions to the smart contract. With each request for a file, ACL-IPFS nodes provide the public key and sign the message using a linked Solana account. This creates a relationship between the nodes and the account, allowing the nodes to use the smart contract to seek and enforce permissions.

Electronic medical records, medical photographs, diagnostic reports, infectious diseases, and other types of data are now more commonly employed in medical care, and a considerable volume of data is generated every day. Infectious diseases can not only be foreseen and planned for protection with good use of this medical data, but they can also be utilized as legal proof for doctors. As a result, it's critical to investigate how to use medical data properly. If the supplied medical data is misused wrongly, the patient's privacy will be jeopardized. As a result, keeping track of the medical data access privileges is a top priority. At this time, Attribute Based encryption (ABE) is the best method for implementing access control. Medical institutions outsource encrypted medical data management to a third party (i.e., a Cloud server), which reduces computing expenses, saves local storage space, and faster data retrieval is also allowed. CP-ABE (Ciphertext-Policy-based Encryption) is a secure way to acquire quick and limited access to data. Furthermore, integrating blockchain technology to modern medical settings has become a new trend, however medical data saved on the blockchain cannot be retrieved efficiently. To solve this challenge, they employ the InterPlanetary File System (IPFS) as our storage platform in [2]. IPFS is a distributed storage protocol that reduces file redundancy. Each stored file is given a unique hash, allowing the user to identify the file by its hash address. Because IPFS is decentralized, there is no single point of failure.

The goal in [3] is to show how to define aliases for addresses in a human-readable manner. The key point is that solutions must be on chains rather than user-defined aliases, which are typically only saved in the user cache. As a result, new wallets, exchanges, and other applications may easily query the blockchain smart contract to acquire a list of all registered aliases. Furthermore, users can utilize the same aliases throughout the ecosystem without having to do any additional work. High costs, long confirmation periods, and a lack of support for autocomplete features are few drawbacks of popular alias solutions. Their solution seeks to address all of the aforementioned difficulties while maintaining a decentralized and permissioned system.

The study [4] aims to assess whether Solana can provide a viable solution to the scalability problem inherent in many existing blockchain networks. Solana positions itself as a platform capable of significantly increasing scalability while maintaining decentralization and security, essential features of blockchain technology. The research collected data from the Solana blockchain over a two-month period, analyzing metrics such as transactions' throughput and fees paid by users for transaction confirmations. The findings indicate that Solana achieves an average transactions' throughput of 2812 transactions per second (TPS) with relatively low transaction fees compared to other blockchain platforms supporting similar functionalities. The study sheds light on Solana's mechanisms, particularly its Proof of History (PoH) consensus, which aims to address scalability without compromising decentralization and security. By providing empirical data and analysis, the research contributes to understanding Solana's potential as a solution to the blockchain scalability problem.

The paper [5] serves as a groundwork on the progressive potential of cryptocurrencies and blockchain innovation, setting the stage for a more profound investigation of Solana's one of a kind commitments to this quickly advancing field. It illustrates the transformative effect of blockchain, emphasizing its decentralized design. Inside this setting, Solana develops as a standout player, advertising novel arrangements to the versatility and execution challenges confronted by existing blockchain systems. Anatoly Yakovenko's groundbreaking work on Solana, especially the presentation of its inventive agreement component based on Confirmation of History (PoH), is highlighted as a key progression. By combining PoS and PoH, Solana accomplishes phenomenal exchange speeds and throughput whereas keeping up decentralization to a critical degree. The proposed framework depicted in the paper [5] diagrams the usage of an e-voting framework utilizing the Solana blockchain. It has subtle elements of the instruments required for advancement, such as the Stay system for Solana's runtime, Rust programming dialect, Hub form director (Nvm), and the Apparition wallet for collaboration with the Solana blockchain. The system's structure is explained, clarifying steps from composing shrewd contracts utilizing Stay to conveying the program and interfacing to a Solana cluster. The voting handle is depicted, counting steps for selecting candidates and confirming exchanges through the Apparition wallet. In general, the proposed e-voting framework on the Solana blockchain illustrates promising execution and unwavering quality for real-world applications.

The paper [6] introduces GreenChain, an operation platform offered on the Solana blockchain and nimble software methodologies. It emphasizes the revolutionary eventuality of blockchain technologies, particularly in decentralized systems, fast data deals, low costs, and security. The authors propose GreenChain for academic and marketable areas, aiming to grease access to scientific content, optimize marketable contracts, and ameliorate translucency and traceability in profitable processes. The operation platform is described as exercising Solana's capabilities for fast, secure, and scalable data deals, eased by its third- generation evidence-of- stake(PoS) terrain and evidence- of- history(PoH) agreement medium. Solana's scalability, security, and decentralization are stressed as crucial features that make it suitable for similar operations. The development process of GreenChain is outlined, including planning, control, construction, and transition stages. The Agile-SCRUM methodology is proposed for incremental development, involving transparent lists of upgrade requests and regular meetings for planning, exertion review, and retrospectives.In conclusion, the paper proposes GreenChain as a result for academic and marketable areas, aiming to ameliorate access to scientific content, optimize marketable contracts, and enhance translucency and traceability in profitable processes. The Solana blockchain and nimble software methodologies are linked as crucial factors in the development and perpetration of GreenChain.

B. Motivation

The motivation for this project likely springs from a desire to overcome the limitations of current centralized file sharing systems. These limitations can put a damper on our ability to freely share information and control our data. One key issue is security. Centralized servers can be vulnerable to hacks, data breaches, and even government surveillance. This raises concerns about the privacy and safety of the information we store on these platforms. Additionally, centralized platforms can restrict access to certain files or even remove them entirely, potentially leading to censorship. Furthermore, centralized systems often struggle with scalability.

As the number of users and the amount of data stored grows, these systems can become sluggish or overloaded. This limits their effectiveness in handling large datasets or supporting a vast user base. This project is motivated by the potential of blockchain technology to address these shortcomings. Blockchain offers a decentralized and secure alternative to traditional file sharing. Data stored on a blockchain is encrypted and distributed across a network of computers, making it highly resistant to tampering and unauthorized access. Additionally, the decentralized nature of blockchain eliminates the risk of censorship from a single entity.

Finally, blockchain technology is known for its scalability, meaning it can efficiently handle a large volume of data and users. By harnessing the power of blockchain, this project aims to create a file sharing system that is secure, censorship-resistant, and scalable. This could revolutionize the way we store and share information online.

C. Problem Statement

Centralized file sharing systems are vulnerable to censorship and corruption. When a single entity controls the system, it becomes easy for governments or other powerful groups to block or manipulate access to certain files.

This has serious consequences for individuals and organizations that rely on these systems to share or access important information.

To overcome these challenges, a decentralized file sharing system leveraging the Solana blockchain and IPFS (Inter Planetary File System) is proposed. By utilizing blockchain technology, the system aims to eliminate the need for centralized control, ensuring a distributed and secure network for file sharing. This approach enhances data availability, and eliminates the vulnerability of a single point of failure. The integration of Solana blockchain and IPFS in the proposed system addresses the limitations of existing file sharing systems, providing a secure, transparent, and scalable platform for efficient and decentralized file sharing.

D. Innovative Content

Blockchain platforms

Blockchain platforms offer a range of services and features, catering to different applications and needs. Here is a brief overview of the blockchain platforms identified:

- Solana : Solana is a high-performance blockchain platform. It is famous for its scalability and low transaction fees. Launched in 2020, Solana uses the concept of a unique intellectual property called Proof of Stake (PoS) and Proof of Stake (PoS) to achieve increased connectivity. If we focus on parallel processing and sharding, Solana has the capacity to handle up to 65,000 transactions per second (TPS). less than $0.01 per transaction Solana, with transaction fees, is popular among developers and users because of its speed, scalability and low cost characteristics.
- Ethereum : Ethereum a well-known blockchain platform, known for the support it gives for smart contracts and decentralized applications (dApps). It introduced the concept of smart contracts, which are self-executing contracts where terms of the agreement are written directly into law. Ethereum's native cryptocurrency, Ether (ETH), is used as fuel for transactions and smart contract creation. Ethereum is widely used for decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and various other decentralized applications.
- Cardano : Cardano is known for its focus on scalability, interoperability and sustainability. Developed by IOHK (Input Output Hong Kong), Cardano aims to provide a secure and highly scalable system for decentralized applications with smart contracts. It uses a proof-stake consensus mechanism called Ouroboros, which ensures energy efficiency and security plays a Cardano multi-layer design separates the settlement ,layer (Cardano Settlement Layer - CSL) from the computation layer (Cardano Computation Layer - CCL), enabling greater scalability and flexibility.
- Avalanche : Avalanche aims to provide a scalable and interoperable ecosystem for building decentralized applications on custom blockchain networks It uses a new consensus protocol called Avalanche, which provides high throughput and fast finality for transactions. Avalanche's architecture supports the development of custom blockchain networks (subnetworks) which can be tailored to specific uses and needs. It provides rich development tools for building decentralized applications and smart contract implementation is also supported.

Each of these blockchain platforms offers unique features and capabilities, addressing different needs and use cases in the rapidly growing blockchain ecosystem Developers and companies can choose a platform,which will suit their requirements and goals to build innovative solutions entrusted to the states.

b. Solana

Solana is a high-performance blockchain launched in 2020, and was developed to solve the scalability issues faced by other blockchain networks, such as slow transaction times and high fees. Solana practices a unique consensus mechanism(method used to achieve agreement, trust, and security across a decentralized computer network.) called Proof of History (PoH) in combination with Proof of Stake (PoS) to achieve extremely high transaction throughput and less transaction fees.

Solana is one among the fastest blockchain networks with over 65,000 transactions happening per second. This transaction rate is attained through parallel processing and sharding. The transaction fee is less than $0.01 per transaction. We can say that solana's popularity is due to its high speed and low-cost transaction fees.

Proof of History (PoH) is a unique consensus mechanism, which gives a way for nodes on the network to agree on the order and timing of transactions, without requiring a large amount of computational power or energy consumption. In addition to PoH, Solana also uses a Proof of Stake (PoS) consensus mechanism that ensures the security and integrity of the network. Validators on the network are required to stake a certain amount of SOL (the native cryptocurrency of the Solana network) to take part in block production and validation. Validators are payed with transaction fees and newly minted SOL for their work in maintaining the network

Solana is currently being used by a number of decentralized applications, including Serum, Mango Markets, Raydium, and Audius. In accordance with the Solana website,currently there are not less than 500 projects building on the Solana blockchain. Solana has achieved over 1 million transactions per second (TPS) during testing, making it one of the fastest blockchain platforms available.

c. Some tools and technologies used to build Solana applications are:

1. Solana Web3.js: It provides an interface used to interact with the solana blockchain.. It allows developers to create, sign, and submit transactions, query blockchain data, and subscribe to events.
2. Solana SDK: a software development kit that gives tools for building and deploying decentralized apps on the Solana network. It includes a command-line interface (CLI) for interacting with the Solana network, a Rust-based programming language, and various libraries for building custom applications.
3. Anchor: This is a framework used for development,that is it is used to build decentralized apps on the Solana blockchain. It provides tools for creating smart contracts, managing state, and building user interfaces. It is built on top of the Solana SDK and it simplifies the process of building and deploying apps on the Solana network.
4. Metaplex: This is a set of smart contracts and tools for building non-fungible tokens (NFTs) and other digital assets on the Solana blockchain. It provides a set of standards for creating and managing NFTs, and also tools for minting, selling, and trading them.
5. SolFlare: This is a web-based wallet and explorer for the Solana network. It allows the users to view their account balances, transaction history, and other blockchain data, It also sends and receives SOL and other tokens.

d. Usage

Solana is currently being employed by a number of decentralized applications, including Serum, Mango Markets, Raydium, and Audius. In accordance with the official Solana website, there are more than 500 projects built on the Solana blockchain currently. Solana has achieved over 1 million transactions per second (TPS) during testing, making it one of the fastest blockchain platforms available.

e. Popularity

Solana has procured exceptional recognition from the cryptocurrency community due to its high throughput and low transaction fees. Solana's native token, SOL, has seen significant price growth in 2021, with a market cap of over $20 billion as of February 2022. Solana has received backing from a number of high-profile investors, including Multicoin Capital, Alameda Research, and Andreessen Horowitz.

f. Future and Position

Solana's high-performance capabilities make it well-positioned to support the decentralized applications in various industries, including finance, gaming, and media. The Solana team has announced plans to launch a decentralized exchange (DEX) and a cross-chain bridge, which could help to further expand Solana's ecosystem and user base Solana is positioned as a competitor to other high-performance blockchain platforms like Ethereum, Polkadot, and Binance Smart Chain, and it shall be interesting to see how these platforms evolve and compete over time. Comparison of existing work with proposed model.(merits , demerits, approach/methodology, along with supporting statistics).

E. Problem Solving

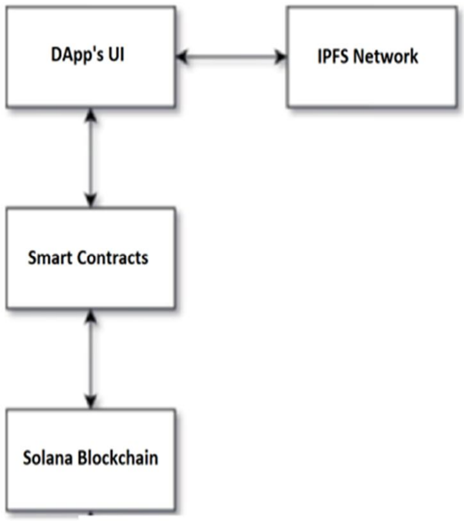
Centralized file sharing systems are vulnerable to censorship and corruption. When a single entity controls the system, it becomes easy for governments or other powerful groups to block or manipulate access to certain files. This has critical issues for individuals and organizations that depend on these systems to share or access important information.

To overcome these challenges, a decentralized file sharing system leveraging the Solana blockchain and IPFS (Inter Planetary File System) is proposed. By using blockchain technology, the system aims to get rid of centralized control, ensuring a distributed and secure network for file sharing. This approach enhances data availability, and eliminates the vulnerability of failure at any single point. Limitations of existing file sharing systems, providing a secure, transparent, and scalable platform for efficient and decentralized file sharing has been addressed in proposed work along with the integration of Solana blockchain and IPFS.

The architecture consists of following components:

1. User Interface: The system includes a user interface that allows the users to interact with IPFS. Users can upload files, retrieve files.
2. Inter Planetary File System (IPFS): IPFS is a decentralized file sharing network that utilizes cryptographic hashes to identify, verify, and transfer files. It employs a distributed hash table (DHT) to store information about file locations and node connectivity. IPFS divides files into smaller chunks. Content IDs are used to identify and retrieve files from IPFS.

System Design



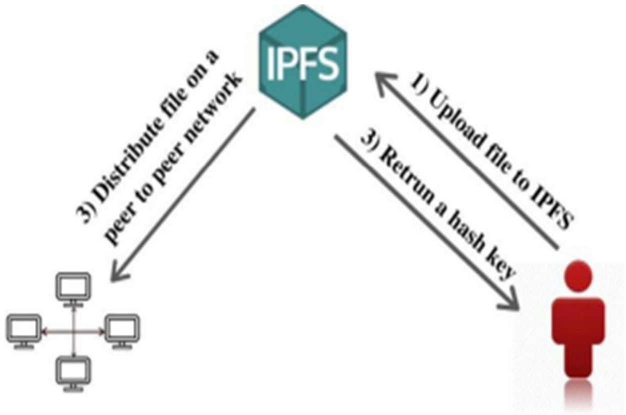


Fig 1 : System Architecture

Fig 2 : IPFS Architecture

3. Smart Contract: A smart-contract is deployed on the Solana blockchain to store and dynamically modify the access control list. The smart contract handles the registration of files, permission management, and validation of access requests.
4. Solana Blockchain: Solana is an open, public blockchain platform that promotes smart contracts,it utilizes "Proof of Stake" and "Proof of History" mechanisms. Solana allows for the creation of transactions, storage of access control lists, and administration of permissions.

Inter Planetary File System (IPFS) as shown in Fig 2 is a peer-to-peer distributed file system. IPFS uses a content-based addressing mechanism. Problem of single point failure can be solved by using IPFS. The advantage of IPFS over a traditional data storage system is that it lacks a central server. Also, data is distributed and stored at different (nodes) on the network. Proposed system uses IPFS to store the data. When a user uploads a file to IPFS that file gets divided into many chunks and stored on all peers of the network. After storing the file, IPFS returns a cryptographic hash key for a specific file.

Implementation

The proposed idea is implemented by dividing the complete tasks into three major units.

1) Connect to Solana Wallet:
   a) The users need to install this as an extension to their browser.
   b) Create an account in a phantom account. When the user uploads a file to the network, a transaction is initiated and some amount of gas fee is deducted from the Phantom wallet automatically. Since DevNet is being used, virtual currency in any amount can be put to the wallet for smooth functioning of this project.
2) File Upload:
   a) Break the file into smaller chunks or divide it into segments.
   b) Generate content identifiers (CID) for each segment using IPFS.
   c) Upload the file segments to IPFS using the IPFS API.
   d) Store the generated CIDs and their corresponding segment information on the Solana blockchain.The users need to install this as an extension to their browser.
3) File Retrieval:
   a) Retrieve the CIDs and segment information from the Solana blockchain.
   b) Use the IPFS to fetch the file segments linked with the CIDs.
   c) Reconstruct the complete file using the retrieved segments.
   d) Utilize Solana's Web3 libraries to work with the smart contracts from client applications.

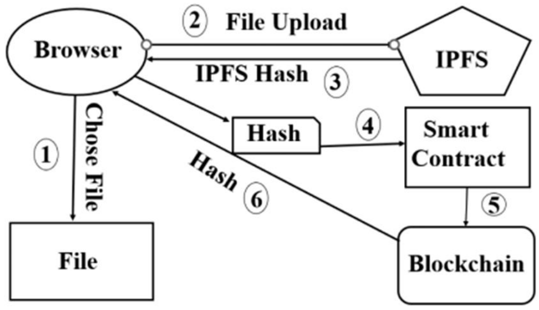


Fig 3 : File Uploading to IPFS and storing hash value in Blockchain

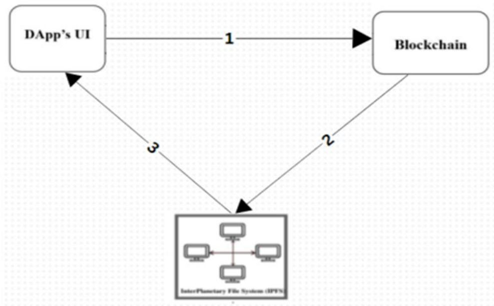


Fig 4 : File retrieving IPFS using Hash saved in Blockchain

File Uploading

The file uploading process is depicted in Figure 3.

1. A file is selected from the DApp (browser).
2. When the DApp form's submit button is clicked, the uploaded file is stored on IPFS.
3. The hash of the file uploaded is returned to the DApp.
4. This hash is the file's location. The file's hash is saved to a smart contract.
5. Which is subsequently kept on the blockchain.
6. Name and Description of the uploaded file are listed on the DApp, from which we can obtain all of the files we have uploaded to IPFS

File Retrieving

The file retrieving process is depicted in Figure 4.

1. When a user selects a file in DApp's UI, request of the CID goes to Solana blockchain.
2. Blockchain sends the requested CID to IPFS.
3. IPFS send the file to DApp's UI

II. CONCLUSION

A decentralized file sharing system that leverages Solana and IPFS combines the advantages of both technologies to create an efficient platform. Solana's high-performance blockchain ensures fast transaction processing and scalability, while IPFS provides a decentralized and distributed file storage solution. By integrating these technologies, users can enjoy secure and censorship resistant file sharing, with files being stored across multiple nodes in the IPFS network and their access permissions managed through the Solana blockchain. This decentralized approach fosters a more resilient and accessible file sharing ecosystem, reducing reliance on centralized servers and enabling seamless sharing of large files across the network.

The future implementations to be incorporated are Making a Searching functionality to fetch files using hash, public address or category. Securing all the programs and converting to mainnet. Making better UI for Writing and uploading data.

REFERENCES

[1] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "BlockchainBased, Decentralized 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), 2018, pp. 1499-1506, doi: 10.1109/Cybermatics_2018.2018.00253.

[2] J. Sun, X. Yao, S. Wang and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," in IEEE Access, vol. 8, pp. 59389- 59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[3] Bodziony, Norbert, Paweł Jemioło, Krzysztof Kluza, and Marek R. Ogiela. 2021. "Blockchain-Based Address Alias System" in Journal of Theoretical and Applied Electronic Commerce Research 16, no. 5: 1280-1296. https://doi.org/10.3390/jtaer16050072.

[4] Giuseppe Pierro, Roberto Tonelli. "Can Solana be the Solution to the Blockchain Scalability Problem?" Conference: 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER).

[5] Hind S. Hassan; Rehab F. Hassan; Ekhlas K. Gbashi,"E-Voting System Using Solana Blockchain" 4th International Conference on Current Research in Engineering and Science Applications.

[6] Adrian Brezulianu, Iolanda Popa, Oana Geman, Iuliana Chiuchisan, Carmen Nastase. "GreenChain:a Solana Blockchain-based Management Platform for Academic/Commercial Areas". November 2022,Conference: E-Health and Bioengineering Conference (EHB).