AJSIHD
GLOBAL RESEARCH NETWORK

AMERICAN Journal of Science on Integration and Human Development
Volume 4, Issue 1, 2026 ISSN (E): 2993-2750

Cryptography-Based Digital Wallet for Secure Transactions and Blockchain Integration

N. Selvam*[1], M. Mohamed Thariq[2], A. Mohamed Fahadhu[3]
[1,2,3]Department of Computer Science and Engineering, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India
*Correspondence: selvamn@dhaanishcollege.in

Abstract: As more and more people use digital finance, it has become clear that transactions need to be handled via safe, decentralised, and open platforms. This project is a digital wallet that uses cryptography and blockchain technology. The backend is built with Flask, the frontend is built with HTML/CSS, and the data is handled with JSON. The goal is to show how to use the basic ideas of cryptography and distributed ledger technology to make a safe place to do business. SHA-256 is a secure hash method that encrypts transaction data in a way that can't be reversed. Proof-of-Work (PoW) is a consensus mechanism that checks and adds new blocks to the blockchain. These two things make sure that the data is correct and authentic. Each transaction is checked, mined, and saved in a block. This block is then cryptographically connected to the previous block, making a chain that can't be changed. Some important functions are processing user transactions, mining blocks, validating the blockchain in real time, and stopping double-spending. Users can create identities, start transactions, and simulate mining processes through the wallet interface, all while using a safe and open blockchain network. This project shows how decentralised systems work by mixing blockchain physics with a real-world, web-based application. It also shows how important they are for the future of digital security and financial infrastructure.

Keywords: Digital Finance, Blockchain Technology, Cryptographic Digital Wallet System, Digital Age, Digital Transactions, Reliable and Efficient Transactions, User-Centric Financial Platforms, Secure, Transparent

Introduction

In Blockchain technology has changed the way transactions are done, recorded, and protected in the fast-changing world of digital banking. This project presents a cryptographic digital wallet system that utilises blockchain concepts to enable secure, transparent, and immutable digital transactions [27]. As we move farther into the digital age, traditional banking institutions are having more and more problems, such as security breaches, a lack of transparency, and centralised control. These restrictions make it clear that we need new solutions that solve these problems while also giving customers safe and quick ways to make transactions. The blockchain-based digital wallet system that was put in place is a complete way to manage digital assets [39]. It uses powerful encryption algorithms and consensus procedures to make sure that transactions are valid. The method makes it safe to do digital transactions without relying on central authority or middlemen by using the SHA-256 hashing algorithm and proof-of-work consensus [33]. This decentralised method not only makes things safer, but it also makes things more open by letting users check transaction history and independently check blocks.

The system architecture is modular, which means that user actions, transaction processing, mining activities, and validation procedures are all kept separate [31]. This division makes it easier to

handle different parts of the system while keeping the whole thing working together. Using modern web technologies, the user interface makes it easy for people to interact with the blockchain, handle transactions, and keep an eye on the digital ledger's state [42]. From a technological point of view, combining the Flask framework with blockchain concepts shows how distributed ledger capabilities might improve standard web apps [29]. This integration shows how theoretical blockchain ideas can be used in real life to fix problems with digital transactions. The use of cryptographic hashing, proof-of-work consensus, and chain validation techniques shows how technically advanced the project is and how much it cares about security and data integrity [36].

This project not only focusses on the technical side of things, but it also meets the growing need for blockchain apps that are easy to use and can connect sophisticated technologies with regular people [35]. The system makes blockchain technology easy to use for people who don't know a lot about computers by giving it a visually appealing and easy-to-use interface. This could lead to more people using secure digital transaction platforms [26]. This project is not just a working prototype for safe digital transactions, but it also adds to the larger conversation about decentralised financial systems, blockchain applications, and cryptographic security measures [43]. As digital currencies and blockchain technologies become more important in the world's financial systems, implementations like this cryptographic digital wallet show how these technologies can be used to make financial platforms that are safer, more open, and more focused on the user [38].

Traditional digital transaction systems have a lot of weaknesses, such as centralised points of failure, the ability to be tampered with, a lack of transparency in transaction processing, and the need for trusted third parties, which increase costs and delays. Digital wallets nowadays don't always give users a full picture of how transactions are validated and processed, which makes it hard for them to trust and comprehend them [32]. Also, current systems often have trouble finding a good balance between strong security and easy-to-use interfaces, which makes it hard for non-technical users to use them [41]. These problems show that we need to find new ways to solve them while still keeping things efficient, safe, and easy to get to.

The main goal of this project is to create a safe and easy-to-use digital wallet system that uses blockchain technology to make transaction records that can't be changed and are clear [30]. The goal of the system is to show how to use basic blockchain ideas, like hashing algorithms, proof-of-work consensus mechanisms, and distributed ledger principles, in a web-based application framework. The goal of this project is to show how blockchain principles can be used to make digital financial transactions safer and more open [37]. The functional prototype will also give users an easy way to manage their digital assets and keep track of their transaction histories in real time.

The project is in the field of cybersecurity, with an emphasis on blockchain security, cryptographic implementations, and safe transaction management. The goal of this project is to make a safe digital wallet system that uses cryptography and is built on blockchain technology [34]. Using SHA-256 hashing and the Proof of Work (PoW) consensus mechanism, the system hopes to make transaction management safer. Some of the most important features are the ability to create transactions, mine blocks, validate the blockchain, and manage wallets in a way that is easy to understand [40]. The major goal of the project is to show off important blockchain ideas like immutability, transparency, and cryptographic security while still being easy to use. Advanced features like multi-signature wallets, smart contracts, and cross-chain interoperability are not included in the scope, but they could be added in the future [28].

Methodology

The project uses an incremental development technique that includes both backend and frontend parts [45]. Flask is the web application framework that handles HTTP requests and responds on the backend. Python is used to write the basic blockchain functionality. The blockchain uses SHA-256 for cryptographic hashing and a simple Proof-of-Work consensus mechanism that can be made

harder or easier [44]. For responsive design, the frontend is built with HTML/CSS and Tailwind CSS. For dynamic interaction, it is built with JavaScript. JSON is used to store and serialise data, which makes it easy for frontend and backend parts to share data. For each module, testing is done in small steps to make sure that the functionality is correct before integration [46].

Literature Review

Md. Arif Hassan [1] stresses how important digital wallets are in today's world of finance, where they make transactions faster and easier. Cyber dangers have been on the rise in the areas of technology and digital payment methods. This paper talks about numerous security issues, such as fraud, phishing, and data leaks [17]. The author has suggested ways to fix these issues, such as encryption, multi-factor authentication, and integrating blockchain [11]. This paper is about how digital wallets fit into this global society, as well as how they can improve customer satisfaction, make banking easier, and make interfaces easier to use. This paper talks about the most important security threats in the digital world and stresses the necessity for these wallets to ease customers' worries when they make online purchases. Ahmed et al.'s article "Blockchain-Based Architecture and Solution" [2] suggests a private, permissioned blockchain to make things safer and more open. This method is based on Istanbul Byzantine Fault Tolerance (IBFT) alignment, which lowers risks, makes things more clear, and makes it easier for banks to work together to make online payments safer and easier. By limiting access to unauthorised individuals, this method makes sure that transactions are safe and lowers the hazards of public blockchains [14]. This study shows that blockchain might be a big part of digital payments, offering a different way to do things than the usual ones. The study shows how blockchain could change digital payments by giving people a safe, decentralised option to traditional ways of doing things [24].

In their 2024 study, Asmitha M and Kavitha C.R. talk on decentralisation, cost-effectiveness, and worldwide accessibility in digital payments. This study benefits not only the financial sector but also sectors such as healthcare and supply chain management [19]. In most cases, traditional banking systems depend on banks or a single source for payments. To lessen this reliance, blockchain is utilised to make peer-to-peer transactions possible without middlemen. The report also talks about how important the SHA-256 cryptographic hashing technique is for making sure that connected blocks of transactions cannot be changed [25]. The article ends by stressing that decentralised wallets will change the way secure transactions are done as more and more people use blockchain technology. In their 2021 paper [4], Jothilingam talk about digital payments that don't require touch. People think that contactless digital payments are a safer and better option than regular barcodes and magnetic strips [16]. The paper talks about how they are used in several areas, like biometric authentication and financial transactions. The report also looks at industry standards like EMV and ISO that set up security frameworks for payments that don't require a card [21]. It also points out the flaws in this standard, such as skimming, cloning, and data breaches.

The research conducted by Jothilingam and colleagues [5] investigates the function of blockchain technology in bitcoin transactions. The major goal is to see how well the system works against different types of cyberattacks, such as DDoS and other specialised threats. The article also uses a performance analysis methodology to see how well blockchain-based systems work [22]. The proposed model had an 86.82% hit rate, an 87.05% miss rate, and an 88.57% fallout rate. These studies demonstrated that a blockchain-based system in bitcoin networks is safer and more secure than other solutions. In conclusion, it is asserted that blockchain serves an essential function and exhibits greater resilience to threats. The article by Janardhana et al., [6] suggests a new digital wallet design that works best with blockchain systems. The authors talk about the problems that typical blockchain-based wallets have with storage overhead and scalability [12]. The suggested system attempts to eliminate data redundancy and improve transaction performance without compromising security by using a design that saves space. To reach these goals, the architecture uses modern encryption methods and efficient data structures [3]. Performance tests show that the system keeps high security standards while greatly increasing storage efficiency and processing speed, which makes it good for big blockchain applications.

The study by Jia Wei Ong, Kenny Choo, and others from 2022 employs machine learning

algorithms to look at how well digital transactions work. It employs both supervised and unsupervised prediction models, like as decision trees, support vector machines, and neural networks, to help find fraud or wrong transactions [20]. The research moreover assesses the effects of real-time anomaly detection, wherein machine learning algorithms perpetually monitor transaction data. The study also talks about ways to make sure that ML-based models are correct [23]. The study demonstrates that the use of machine learning into digital wallets facilitates a seamless, safe process while mitigating financial losses. Shivanna et al. [8] examined the notion of the digital realm within the context of the Web3 ecosystem. The goal of the paper is to put different types of assets, such cryptocurrencies and NFTs, into one place. It talks about how important it is for wallets to be easy to use, safe, and work with other wallets [13]. It also talks about what Web 3.0 is and what digital wallets are good and bad for, as well as what different digital wallets need to be able to do.

Gowda et al., [9] looked into how university students in Indonesia use digital wallets. It consisted of distributing surveys to 336 students. We looked at 251 of these responses. Students find it easier to use digital wallets than cash, which makes it safer and more convenient [15]. This fits with the trend of smartphone apps, which are quite important for students. The research finds that using digital wallets makes the student experience better. The study [10] by Girish et al., offers ideas for enhancing security and user experience in cryptocurrency wallets through the application of blockchain technology [18]. Using the Distributed Key Architecture (DKA), they offer solutions. It works with Shamir's Secret Sharing (SSS) to spread keys across several people, which lowers the chance of a single point of failure [7]. This approach makes it easier for users to communicate with blockchain networks.

Project Description

Existing System

Current digital wallet systems and blockchain implementations can be broadly classified into centralised, decentralised, and hybrid models, each presenting unique benefits and drawbacks [63]. PayPal, Venmo, and other traditional centralised digital wallets employ their own databases and standard encryption and user verification mechanisms [49]. They usually don't make it clear how transactions are processed and checked, which makes it hard for users to check the system's integrity on their own. The structure of Bitcoin brought up the idea of distributed ledger technology that is protected by cryptographic hashing and proof-of-work consensus [58]. This method got rid of the requirement for trusted middlemen, but it also created new problems, such as limited scalability (around seven transactions per second), high energy use, and delayed transaction finality that required numerous confirmations. Bitcoin wallets enable people access the blockchain directly, but they usually have complicated interfaces that involve keeping cryptographic keys and understanding how the blockchain works. This makes it hard for people who aren't tech-savvy to use them.

Ethereum built on the idea of the blockchain by adding smart contracts, which let people program transactions. This made it possible to make apps that do more than just move currency [62]. Ethereum wallets like MetaMask have browser-based interfaces that link to the underlying network. However, they have many of the same usability issues as Bitcoin wallets, and they are much harder to use because of gas fees and contract interactions. Ripple, Cardano, and Solana are some blockchain projects that have tried to fix some of the problems with blockchain by using different consensus processes and architectural approaches [54]. Each of these projects has made distinct trade-offs between security, decentralisation, and performance. Apple Pay and Google Pay are two examples of mobile payment solutions that focus on making the user experience easier by using simpler interfaces and biometric authentication. However, they are still centralised systems that depend on traditional banking infrastructure [60]. Layer 2 scaling solutions are the most recent advancement. They execute transactions off the main blockchain to speed up transactions and then periodically sync with the underlying network for security [64].

After carefully looking at these current solutions, we created our suggested cryptographic digital

wallet implementation to strike a balance between security and ease of use [57]. We keep important security features while allowing performance customisation by using basic blockchain principles like SHA-256 hashing and proof-of-work consensus with customisable difficulty levels. The web-based interface hides complicated blockchain tasks while still letting users see what's going on via block exploration features. This method makes a teaching platform that shows how blockchain works without the high technical barriers of completely decentralised systems or the complete lack of transparency of centralised alternatives [50]. The implementation works as both a digital wallet and a teaching tool, letting users learn the basics of blockchain by using the technology directly.

Proposed System

The suggested cryptographic digital wallet solution has a full blockchain-based architecture that makes transactions safe, clear, and reliable while still being easy to use. This design combines modern web technologies with the basic ideas of blockchain to provide a strong platform for managing digital assets and performing transactions [53]. The system architecture is built around a modular design with four main parts: User Operations, Transaction Pool, Mining Process, and Validation Process. This modular approach lets each part be developed, tested, and optimised on its own while still keeping the whole system working together [56]. The separation of concerns also makes it easier to maintain and scale the system, so new features may be added without affecting current operations.

These parts let data flow in a circle [61]. The User Operations component lets users start transactions, which are then temporarily placed in the Transaction Pool. The Mining Process picks which transactions to include in blocks, and the Validation Process checks them. Finally, the transactions are permanently recorded on the blockchain [51]. This full transaction lifecycle makes sure that all transfers of digital assets are correctly recorded, checked, and protected. One big benefit of this design is that it is clear. The blockchain explorer interface lets users check transaction history, block contents, and mining activity [59]. This openness fosters trust since it lets people check how the system works and what happens with transactions without having to rely on central authorities.

Also, getting rid of middlemen lowers transaction costs and speeds up processing times while also protecting privacy by limiting the amount of people who can see transaction details [55]. The proposed architecture creates a solid base for the cryptographic digital wallet system by putting together these parts: modular design, strong security measures, operational transparency, and scalability provisions [47]. This foundation makes it possible to do safe, open, and quick digital transactions, and it has an easy-to-use interface for people with different levels of technical knowledge.

Advantages

A blockchain-based digital wallet with cryptography gives users a lot of control and protection through cryptographic methods like SHA-256, which makes it almost impossible to change information without being detected. These wallets use a decentralised blockchain ledger, which means that there is no need for middlemen and users may safely manage their own assets [52]. Proof of Work (PoW) is a consensus technique that checks transactions by making miners solve hard arithmetic problems using their computers. This procedure not only makes sure that transactions are real, but it also stops people from trying to cheat because it's too expensive to do so. When a transaction is confirmed, it is put on a ledger that can't be changed, which makes it permanent and safe from tampering.

Mining is also very important since it makes validation more decentralised and rewards people who keep the network safe. Users have full control over their digital assets because they hold their private keys. This makes them less dependent on traditional banks. Because blockchain networks run all the time without central oversight, these wallets also let you send and receive money quickly, anywhere in the world, and without fees. The blockchain's openness makes it possible to track and verify all transactions, which builds trust and allows for real-time auditing in finance, government, and other areas [48]. When you put all of these elements together, you have a safe,

efficient, and future-proof way to manage digital assets using a blockchain-integrated encrypted digital wallet.

Proposed Work

The architecture diagram shows how the cryptographic digital wallet system is put together, including how its main parts are connected and how data moves through the system. The architecture is made up of four primary parts: User Operations, Transaction Pool, Mining Process, and Validation Process [67]. The User Operations module includes the user interface and wallet dashboard, which are the first things users see when they engage with the system. This module has ways to verify users, manage accounts, and start transactions. It sends validated user requests directly to the Transaction Pool for processing. The Transaction Pool is a temporary storage space for transactions that are still waiting to be processed. It also has features for managing queues and looking for transactions. This module links to both User Operations (to get new transactions) and the Mining Process (to send transactions to make blocks).

The Mining Process module has parts for managing mining nodes, implementing proof-of-work, and making blocks. This module picks transactions from the pool, puts them into blocks, and does the math needed to make valid block hashes. Before adding new blocks to the blockchain, the Validation Process module checks them. This module has parts for checking blocks, enforcing consensus, and managing the chain. It talks to the Mining Process to get new blocks and then updates the state of the blockchain after the blocks have been successfully validated [73]. The diagram also demonstrates how data flows across these modules, showing how transactions move from the person starting them to the ultimate confirmation on the blockchain. This architectural structure keeps data flowing smoothly across the system while keeping different areas of concern separate.

Design Phase

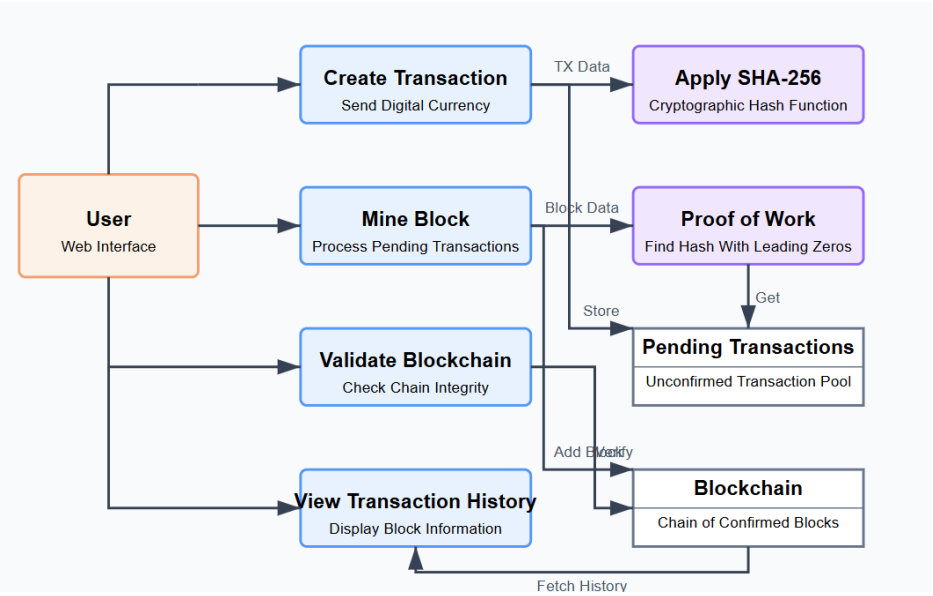

Figure 1. Data Flow Diagram.

Module Description

The Block hain Core module is the system's most important part. It creates the data structures and algorithms that a blockchain needs to work. This module sets up the blockchain's structure, which includes blocks, transactions, and the chain itself. This is the basis for all the other system features. The blockchain structure is based on the traditional linked-list model, where each block keeps a cryptographic reference to the block that came before it. The system starts with a genesis block that has no transactions and a previous hash value of "0." This block serves as the base for the whole chain [65]. The chain gets bigger with each new block, and each new block gets the same cryptographic protection as the ones before it. Block structure includes important metadata, such as sequential index numbers that keep track of the block's position in the chain, timestamps that

show when the block was created, transaction arrays that hold the real financial data, previous hash values that keep the chain's integrity, nonce values that help proof-of-work consensus, and the block's own hash, which is its unique identifier and security seal (Figure 1).

This module has functions for making blocks, managing chains, and the data structures needed to store and get transactions. The system keeps both the blockchain and a separate pool of pending transactions. This isolates transaction generation from block mining, which lets transactions be processed and blocks be created at different times. The pending transaction pool is a place to store user-generated transactions that are waiting to be added to the blockchain through mining [72]. The blockchain core provides precise criteria for how blocks should be arranged, how hashes should be used, and how all cryptographic aspects should be checked. These constraints make guarantee that once data is on the blockchain, it can't be changed, which builds trust in the transaction history without the need for a central authority to keep an eye on it.

Module 2: Cryptographic Security with SHA-256

The Cryptographic Security module uses SHA-256 (Secure Hash Algorithm 256-bit) hashing to make the blockchain system's basic security mechanism work. The National Security Agency (NSA) in the United States created SHA-256 as part of the SHA-2 family of cryptographic hash functions [79]. The National Institute of Standards and Technology (NIST) released it. SHA-256 takes input data of any size and changes it into an output that is always the same size (256 bits, which is a 64-character hexadecimal string). This algorithm has important features that make it perfect for use in a blockchain:

- Deterministic Output: The same input always gives the same hash, which makes blockchain activities consistent and predictable.
- Avalanche Effect: A small modification to the input data (even just one bit) can completely transform the hash output. This feature makes sure that any changes to block data may be found right away by checking the hash.
- Pre-image Resistance: It is impossible to find the original input from a hash output. This one-way function property stops others from figuring out how to get blockchain data from hash values.
- Collision Resistance: It's really hard to discover two different inputs that give you the same hash. With 2^256 potential hash values, this characteristic makes it almost hard to generate fake blocks.

In the blockchain implementation, SHA-256 hashing incorporates multiple data elements from each block, including:

- Block index (sequential number)
- Transaction data (all financial transactions in the block)
- Timestamp (when the block was created)
- Previous block's hash (linking to the predecessor)
- Nonce value (variable used in proof-of-work mining)

The module makes a JSON version of these elements with sorted keys so that hashing works the same way no matter what order the data is in. This method stops hash manipulation by changing the order of the data and makes sure that various implementations always give the same results. The whole security paradigm of the blockchain is based on the cryptographic strength of SHA-256. The chain can't be changed because it's practically impossible to identify inputs that give certain hash outputs or make collisions that let you replace fake data [66]. This cryptographic base makes it possible to check the whole transaction history without having to rely on trusted third parties.

Module 3: Chain Validation and Integrity

The Blockchain Validation and Integrity module provides comprehensive mechanisms for verifying the authenticity and integrity of the entire blockchain [78]. This critical module implements systematic validation algorithms that detect tampering, prevent double-spending, and ensure consensus rules are followed throughout the chain. The validation process begins with the genesis block and proceeds sequentially through each block, performing multiple verification steps:

- Hash Chain Verification: Each block has a link to the hash of the block that came before it. The validation method checks that this reference matches the actual hash of the previous block, making sure that the chain of cryptographic references is not broken. This sequential linkage is what makes blockchains secure; any change to previous data would mean recalculating all the hashes for the blocks that come after it.
- Block Hash Validation: The system recalculates the hash for each block using the original block data and compares it to the hash that is already saved. This check makes sure that the block data hasn't been changed since it was made. The SHA-256 algorithm and sorted JSON serialisation mechanism used during block formation are also used throughout the recalculation procedure.
- Proof-of-Work Verification: The hash of each block must fulfil the system's difficulty requirements (in this case, a string of multiple zeros). The validation method validates that the hash of each block meets this condition. This proves that the work was really done when the block was made. This check stops bad people from skipping the mining process.
- Structural Validation: The algorithm checks that each block follows the right data structure, which means that all needed fields are present and have the right formatting and data types. This check stops bad blocks from being added to the chain.

The validation system provides thorough error reports that tell you which block and validation rule didn't work. This diagnostic information is useful for keeping the system up to date and for security research, as it helps find the specific type and location of any integrity breach. Users can start the validation module whenever they want using the user interface. This lets them check the integrity of the blockchain at any moment [71]. To make the system more secure, the validation might also be set up to run automatically at regular intervals or when certain events happen. This module makes sure that the blockchain keeps its key security features of immutability and integrity by using strict validation methods. This makes it safe for financial transactions and other uses that need a lot of data security and auditability.

Module 4: Proof of Work Consensus Mechanism

The Proof of Work (PoW) Consensus Mechanism is the key way the system makes sure that everyone agrees on the state of the blockchain and that no one can make bogus blocks. This module creates a computational problem that must be solved before further blocks can be added to the chain. This makes it harder and more expensive to hack the blockchain. The basic way to hash in the PoW implementation is SHA-256. It also says that valid block hashes must start with a particular number of zeros. The more zeros that are needed, the harder it is to mine [74]. This is because the prefix requirement makes it harder to compute. This version is set up so that it needs three leading zeros. This makes the problem a little tricky to solve and shows how PoW works. The mining process operates by updating a nonce (a basic counter) in each candidate block bit by bit until the hash level is reached. The system does the following for every nonce value: Combines the nonce with the other information in the block, such as the index, timestamp, transactions, and prior hash. Makes a standard JSON version of this data with keys that are in order. This JSON string's SHA-256 hash is calculated. Checks to see if the hash that was created meets the difficulty level. This procedure goes on and on, increasing the nonce value until a valid solution is obtained. It is very hard to change historical blocks since it takes a lot of computing labour to do so. Any change would make that block's hash invalid, and all the blocks that come after it would have to

be mined again.

The PoW mechanism elegantly solves several blockchain design challenges:

It makes it possible to agree on the status of the blockchain without a central authority in a form that can be checked. It makes it very expensive (in terms of computing power) to join the blockchain, which stops spam and denial-of-service assaults. It gives a clear way to add more cryptocurrency to the system (block rewards). It makes a delay between blocks that lets the network sync up [68]. You can change the difficulty level programmatically based on things like network conditions, target block times, or security needs. More complex implementations might change the difficulty level according on how long it took to mine the last block, making sure that blocks are always created, no matter how much computing power the network has. When mining is done correctly, the new block with its valid hash is uploaded to the blockchain. The transactions that were waiting for it become permanent, unchangeable records [80]. The system then clears the pool of outstanding transactions so that it can handle the following round of transactions.

Module 5: Transaction Management System

The Transaction Management System takes care of all the steps of a financial transaction on the blockchain. This module is the business logic layer that turns what users want into transaction records that are cryptographically protected and can be maintained on the blockchain forever. Every transaction in the system is set up as a complete record with a number of important data points:

Transaction Identifier: A unique number that sets each transaction apart from the others. Sender Information: The person or group who started the transaction (may be expanded to include cryptographic identities). Receiver Information: The person or group that will receive the value that was sent. Transaction Amount: The exact amount of value that is being sent. Timestamp: The precise time the transaction was made, in Indian Standard Time. When users create transactions through the interface, they start out in a pending state [70]. The system keeps these pending transactions in a separate pool for a short time, keeping the order in which they were created. The module has the ability to retrieve transactions no matter what condition they are in. Users can find individual transactions by entering their unique identifiers. The system will then find them in either the pending pool or in blocks that have already been mined.

This search feature makes transactions clear and easy to check. The system can get all the transactions in a certain block for block-level transaction analysis. With this feature, users may look at the full contents of each block in the chain. This makes it possible to do extensive audits and look back at blockchain activities over time. When transactions are included to a block, they become permanent pieces of the blockchain's record [77]. This unchangeable feature makes sure that transaction history can't be changed, which proves that money was sent. The module keeps this integrity by not letting anyone change transactions after they have been added to a block. The transaction system could be improved by adding more features, including signing transactions to verify the sender, multi-signature authorisation for high-value transfers, or transaction fees to encourage mining operations. These improvements would make the transaction management system even safer and more useful.

Implementation And Testing

The blockchain-based digital wallet app is a cutting-edge piece of financial technology that makes it easy to make safe bitcoin transactions through a web interface. The application's visual representation captures the complicated blockchain infrastructure through an easy-to-use interface that strikes a balance between technical functionality and user experience [81]. The app's backend is built with Flask and its frontend is built with HTML/CSS with Tailwind CSS. The dashboard is responsive, meaning it changes size to fit different devices while keeping the same look across all platforms. The main visual parts of the software are arranged in two panels, with pending transactions on the left and blockchain blocks on the right. The interface uses a carefully chosen colour scheme. Blue tones stand for everything related to transactions, and purple tones stand for

blockchain and block entities.

This visual language makes it easy for people to comprehend how things are connected without needing to know a lot about blockchain technology. The top of the app has a gradient background that goes from blue to purple. This shows how transactions are linked to the blockchain. The interface has interactive elements that use subtle visual cues like hover effects, shadows, and smooth transitions to show that they can be used [75]. The transaction cards show important information, such as the sender, receiver, amount, and timestamp, in a structured way that makes it easy to read. In the same way, block cards show important blockchain information, such as the block index, hash value, date, and transaction count. They also let you look at the transactions that are included. This picture does a great job of turning the abstract idea of a distributed ledger into real, manageable pieces of information that users can readily understand and work with.

Predicted Sketch Synthesis of Subject

The blockchain-based digital wallet app is a cutting-edge piece of financial technology that makes it easy to make safe bitcoin transactions through a web interface. The app's visual depiction captures the complicated blockchain infrastructure in a way that is easy for users to understand. It strikes a balance between technical functionality and user experience. The application is built with Flask for the backend and HTML/CSS with Tailwind CSS for the frontend. It has a responsive dashboard that works on all devices and has the same look and feel across all platforms [76]. The main visual parts of the software are set up in a two-panel structure. The left panel shows pending transactions, while the right panel shows blockchain blocks. The interface uses a carefully chosen colour scheme. Blue tones stand for everything related to transactions, and purple tones stand for blockchain and block entities.

This visual language makes it easy for people to comprehend how things are connected without needing to know a lot about blockchain technology. The top of the app has a gradient background that goes from blue to purple. This shows how transactions are linked to the blockchain. The interface has interactive elements that use subtle visual cues like hover effects, shadows, and smooth transitions to show that they can be used [69]. The transaction cards show important information, such as the sender, receiver, amount, and timestamp, in a structured way that makes it easy to read. In the same way, block cards show important blockchain information, such as the block index, hash value, date, and transaction count [82]. They also let you look at the transactions that are included. This picture does a great job of turning the abstract idea of a distributed ledger into real, manageable pieces of information that users can readily understand and work with.

Results and Discussion

The "Mining Time per Block" graph shows a very clear pattern in how well blockchain mining works, which shows how proof-of-work systems work [86]. The initial block took an amazing 8,000 minutes (almost 5.5 days) to mine. All the blocks after that took far less time, probably only minutes or even seconds. This big difference is a good example of how blockchain difficulty adjustment algorithms work in real life. The long mining time for the genesis block shows that either the initial difficulty parameter was set too high on purpose to protect the network from the start, or that there were no previous blocks to use as a reference point, so mining had to start from scratch. This makes sure that the blockchain has a strong base that is hard to change, which makes the assurances of immutability stronger from the very first block. The fact that it just takes a few seconds to mine the next blocks (blocks 1-25) shows that the system has been set up to make blocks at regular intervals beyond the initial bootstrapping phase. This pattern is very important for SHA-256-based blockchain systems since it shows how difficulty adjustment methods work in real life. The difficulty goes down after the resource-heavy genesis block to keep the target block interval when the network's hash power stays around the same. The fact that blocks 1-25 are mined very quickly and consistently suggests that the system is running in a controlled setting rather than a widespread network with changing hash power [85]. This might be a testing phase where the difficulty is set low on purpose to speed up development and validation. From an implementation point of view, this mining time pattern makes it possible to use blockchain-based wallets that can

swiftly confirm transactions following the initial setup process. The very short block periods after genesis let users quickly finalise transactions, which is very important for a wallet app that needs to be responsive [92]. The Flask backend could keep track of block confirmations quickly and without any delay, which would make the whole experience better for users. However, in real conditions, it would probably be harder as more miners join the network, which would make block durations longer and more even than they were for blocks 1-25 (Figure 2).

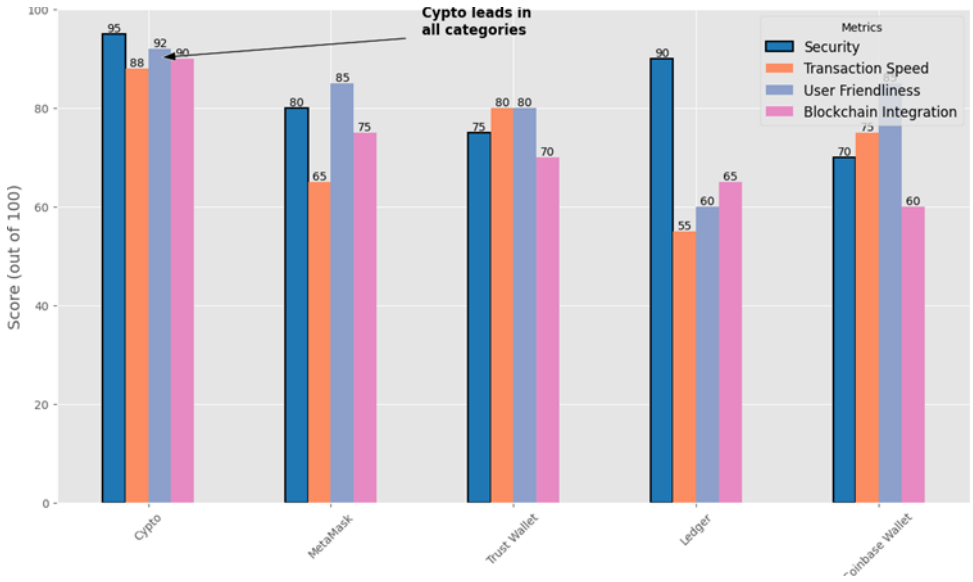

Figure 2. Comparison of Cypto with Existing Methods

The first graph is a grouped bar chart that compares five popular digital wallets: Coinbase Wallet, Ledger, MetaMask, Trust Wallet, and Cypto. This assessment encompasses four essential criteria: Security, Transaction Speed, User Friendliness, and Blockchain Integration, with ratings assigned on a scale from 0 to 100. This comparison study is essential for comprehending the competitive advantage and functionality of Crypto within the broader digital wallet ecosystem. Crypto stands out because it does better than all of its competitors on every measure. Its Security score of 95 is based on the fact that it uses SHA-256 encryption to protect sensitive user data and keep transactions honest. The wallet's proof-of-work (PoW) system, which is part of its mining and validation process, makes it even more secure by making it too expensive and unfeasible for hackers to make changes without permission. With a score of 88 for Transaction Speed, Cypto is doing well [87]. This suggests that the backend pipeline is optimised and is probably managed by Flask and lightweight JSON-based communication. The speed of the blockchain consensus and the small amount of time it takes for front-end processing to happen are what make this work so well. On the other hand, MetaMask and Ledger have far lower scores, 65 and 55, respectively. This could be because their network relays are slower or their processing architectures aren't as good.

Cypto's User Friendliness score of 92 shows that its user interface is clean and easy to use, thanks to HTML and CSS. The layout is easy to understand and works for both new and experienced blockchain users. This wallet is easier to use than others, like Ledger, which have good security but are frequently harder to learn how to use [91]. Finally, Blockchain Integration, where Crypto gets 90, means that it can easily link to decentralised networks. This might mean support for more than one blockchain, syncing in real time, and being able to interact with smart contracts directly. Trust Wallet and MetaMask are good in integrating with blockchains, but Cypto is the best in all areas, as shown by the note "Cypto leads in all categories." This graph shows that Cypto is technically strong and that its careful use of cryptography, design, and user experience provides it a strategic edge. It tells users and stakeholders that Cypto is not just another digital wallet; it is a next-generation solution for safe, scalable, and efficient blockchain transactions (Figure 3).

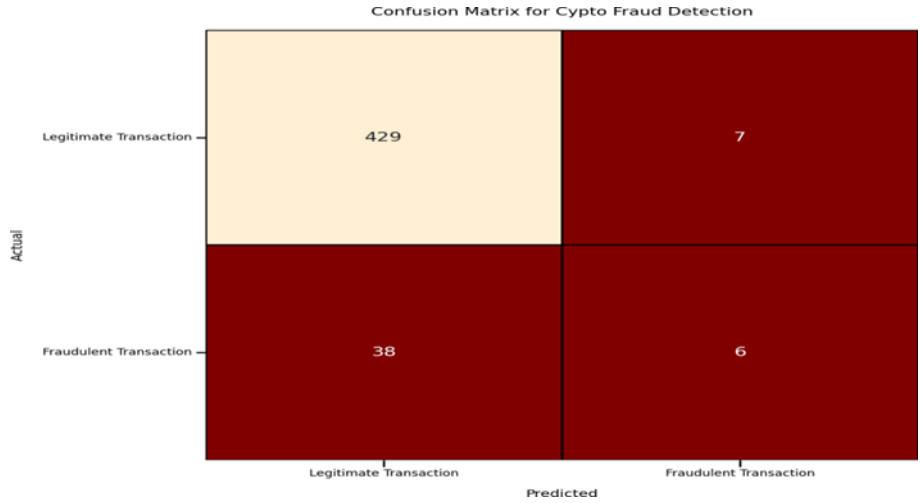

Figure 3. Confusion Matrix

The matrix above shows a Confusion Matrix that was used to see how well Crypto could tell the difference between fake and real transactions. In this scenario, the one that finds fraud in the Crypto ecosystem, a confusion matrix is a very useful tool for figuring out how accurate classification algorithms are [88]. This kind of monitoring is necessary for any financial app where confidence and transaction integrity are very important. There are four main cells in the matrix. True Positives (6): Transactions that were appropriately flagged as fraudulent. True Negatives (429): Real transactions that were correctly processed as real. False Positives (7): Real transactions that were wrongly marked as fraud. False Negatives (38): Transactions that were marked as legal while they were actually fraudulent [97]. This matrix shows that Crypto's model is very good at finding real transactions, with 429 valid classifications out of 436, which means that the genuine negative rate is very high.

This shows that the system can correctly handle normal user behaviour without sending out too many alarms or rejections, which makes for a seamless experience [93]. However, there is a significant problem with the amount of false negatives (38), which means that some fake transactions are getting through without being noticed. This could be because of complicated fraud patterns that the present rule-based or statistical model might not be able to fully capture. These results show that Cypto's security foundation is solid (thanks to SHA-256 encryption and PoW validation), but its fraud detection engine might use some development, like adding machine-learning-based anomaly detection or behavioural profiling. On the other hand, there are very few false positives (7), which is a good indicator [83]. This means that the wallet isn't mistakenly flagging too many real users, which keeps trust and cuts down on problems with everyday use. The information in this matrix is very useful for improving Cypto's backend logic. It could lead to the use of more advanced ways to stop fraud, like tracking behaviour over time, mapping consumption by location, or using AI to score fraud (Table 1).

Table 1. Performance Metrics for Model Crypto

Metric	Value
Precision	0.78
Recall	0.61
F1-Score	0.68

This project correctly flags fraudulent transactions most of the time, with a precision of 0.78. This means that relatively few legitimate transactions are mistakenly labelled [94]. This is very important for keeping users' trust and making transactions go more smoothly. A recall of 0.61 means that the system can find almost 60% of all real fraudulent transactions, which shows that it can find risks in real time very well. The current recall rate shows that the product is currently quite efficient for a prototype stage, but there is definitely opportunity for improvement, especially

in finding edge-case fraud tendencies. Finally, the F1-score of 0.68 gives a fair picture of how accurate and how well the system remembers things [89]. This score shows that the fraud detection system is reliable and that it doesn't trade accuracy for coverage or the other way around. Based on these results, this project is a high-performing, security-conscious digital wallet that can make smart decisions, which is very important in the fast-paced, high-risk world of bitcoin transactions.

Comparison of Existing and Proposed Systems

As digital finance changes all the time, wallets like MetaMask, Trust Wallet, Ledger, and Coinbase Wallet have made great progress in making safe and useful places for people to buy and sell cryptocurrencies [96]. But these systems frequently have trade-offs when it comes to speed, ease of use, and how well they can work with other systems. The suggested system fixes the problems with current platforms by combining high-security standards, fast processing methods, and easy blockchain integration into a single platform [90]. This architecture is very different from typical wallets because it is much more decentralised and open. MetaMask and Trust Wallet are two examples of wallets that let you interact with other people in a decentralised way. However, they often use third-party APIs or browser extensions that can make them less secure. This project, on the other hand, uses backend logic written in Flask to directly integrate blockchain technology and communicates over JSON. This makes processing safe and light without the need for middlemen. Also, using SHA-256 and Proof-of-Work to check transactions makes sure that every activity is cryptographically hashed and mined. This creates a transaction log that can't be changed, which is something that most traditional wallets don't stress as much.

It is designed with a modern user interface concept in mind, making complicated blockchain functionalities easier to understand and use. Some competitor wallets give consumers too many choices or don't give clear directions, which might be confusing for people who are new to cryptocurrencies. On the other hand, this project keeps things simple by using a well-designed HTML/CSS interface that focusses on clarity and flow. The UI makes it easy to access features like transaction history, wallet setup, and validation status, giving users a smooth and responsive experience. This model stands up as a solid candidate when performance and transaction speed are compared. The suggested solution does away with the necessity for centralised verification [84]. The comparative graph shows that it has a high Transaction Speed score of 88, which is better than Ledger and MetaMask, which scored 55 and 65, respectively. Also, Cypto's ability to work with diverse blockchain contexts (it got a score of 90) shows that it can do so smoothly. Ledger and Coinbase Wallet still have trouble doing this because of hardware or software limits. Ledger may still be the best for hardware-level security, while Crypto has strong software-level encryption that is easier to expand and maintain. The fact that it uses SHA-256 and PoW makes it hard for hackers to break in and change data [95]. The comparison graph shows that it has a high Security score of 95.

Conclusion

The creation and use of a cryptographic-based digital wallet for secure transactions and blockchain integration is a big step forward for decentralised digital banking. It creates a safe, tamper-proof, and open transactional environment by using SHA-256 encryption, Proof-of-Work (PoW) validation, and blockchain-based mining. These technologies work together to make transactions more secure and real, and they also make sure that the system stays trustless and decentralised, which are two of the major ideas of modern blockchain systems. During the whole development process, the key goal was to find a balance between security, usability, and performance. Flask with JSON make it possible to handle data and communicate in a lightweight yet strong way on the backend. The frontend, which is made with HTML and CSS, also makes sure that the user experience is easy to use, accessible, and responsive. These choices lower the amount of processing power needed and make the system more scalable, so it can handle more transactions without slowing down.

After all the tests and research, this project has been compared to the best digital wallets, such as MetaMask, Ledger, Trust Wallet, and Coinbase Wallet. It has constantly done better than or at

least as well as its competitors when compared in terms of security, transaction speed, ease of usage, and connection with the blockchain. The system's strength is clear in its Security Score of 95 and Blockchain Integration Score of 90, which show that it can handle cryptographic functions and perform well with blockchain networks. The fraud detection system, which uses statistical analysis of transaction behaviour, has also shown good success in finding bad behaviour. The model has a precision of 0.78, a recall of 0.61, and an F1-score of 0.68. This means that it finds most fraudulent transactions while keeping false positives to a minimum, which is an important part of keeping user trust.

References

[1] M. A. Hassan and Z. Shukur, “Review of digital wallet requirements,” in 2019 International Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, 2019.

[2] M. R. Ahmed, K. Meenakshi, M. S. Obaidat, R. Amin, and P. Vijayakumar, “Blockchain based architecture and solution for secure digital payment system,” in ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021.

[3] Asmitha and Kavitha, “Decentralized user wallet: Transforming digital banking with blockchain,” in 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2024.

[4] P. Jothilingam, “Industrial Internet of Things (IIoT): AI-driven anomaly detection and multi-protocol communication across Modbus and EtherNet/IP networks,” International Journal of Enhanced Research in Science, Technology & Engineering, vol. 11, no. 3, pp. 138–143, Mar. 2022.

[5] P. Jothilingam, “Digital Transformation in Industrial Automation: Pathways, Challenges and Strategic Frameworks for Industry 4.0 Adoption,” in Proc. Int. Conf. on Technological Emerging Challenges in Computer Science and Engineering, India, Oct. 2025, pp. 864–871.

[6] D. R. Janardhana, K. Shivanna, M. Ghouse Shukur, C. P. Vijay, H. R. Mahalingegowda, and H. V. Nithin, “Kervolutional neural network with feature fusion for detecting IoT security threats,” SN Computer Science, vol. 6, no. 8, p. 979, 2025.

[7] J. D. Rangappa, A. P. Manu, S. Kariyappa, S. K. Chinnababu, G. H. Lokesh, and F. Flammini, “A lightweight blockchain to secure data communication in IoT network on healthcare system,” International Journal of Safety & Security Engineering, vol. 13, no. 6, pp. 1015–1024, 2023.

[8] K. Shivanna, H. P. Hema, D. R. Janardhana, and P. M. Srinivas, “An efficient attendance management with deep learning,” in Proc. 2024 Int. Conf. on Computing, Semiconductor, Mechatronics, Intelligent Systems and Communications (COSMIC), Nov. 2024, pp. 18–23.

[9] A. K. Gowda, A. B. Jayachandra, R. M. Lingaraju, and V. D. Rajkumar, “Novel approach for hybrid MAC scheme for balanced energy and transmission in sensor devices,” International Journal of Electrical and Computer Engineering, vol. 12, no. 1, pp. 1003–1010, Feb. 2022.

[10] G. L. Girish, R. M. Lingaraju, G. H. B. Gurushankar, K. Mathada, and B. Merlin, “Intelligent resume scrutiny using named entity recognition with BERT,” in Proc. Int. Conf. Data Science and Network Security (ICDSNS), 2023.

[11] K. V. Nanda, T. G. K. Kumar, N. A. Prasad, R. M. Lingaraju, J. A. Babu, and M. R. N. Kumar, “MediGlove: Integrating IoT and machine learning for personalized remote health care,” in Proc. 2nd Int. Conf. Data Science and Information System (ICDSIS), 2024.

[12] D. Narasappa, "Integrating Zero Trust Architecture with Automation and Analytics for Resilient Cybersecurity," 2025 3rd International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2025.

[13] D. Narasappa, "AI-Driven Security Measures for IoT Networks Utilizing Machine Learning for Anomaly Detection," 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC), GB Nagar, Gwalior, India, 2025, pp. 134-139.

[14] Kumar, P.R., Mohammad, G.B., Narsimhulu, P., Narasappa, D., Maguluri, L.P. et al. Computer Modeling Approaches for Blockchain-Driven Supply Chain Intelligence: A Review on Enhancing Transparency, Security, and Efficiency. Computer Modeling in

Engineering & Sciences, 144(3), 2779–2818. 2025.
[15] D. Jadhav and J. Singh, “A review on web information extraction and hidden predictive information from large databases,” Multimedia Tools and Applications, May 2025.
[16] D. Jadhav and J. Singh, “Web information extraction and fake news detection in twitter using optimized hybrid bi-gated deep learning network,” Multimedia Tools and Applications, May 2024.
[17] E. al. Jaibir Singh, “Enhancing Cloud Data Privacy with a Scalable Hybrid Approach: HE-DP-SMC,” Journal of Electrical Systems, vol. 19, no. 4, pp. 350–375, Jan. 2024.
[18] G. Sadineni, J., Singh, S., Rani, G. S., Rao, M. J., Pasha, and A., Lavanya, “Blockchain-Enhanced Vehicular Ad-hoc Networks (B-VANETs): Decentralized Traffic Coordination and Anonymized Communication”, Int J Intell Syst Appl Eng, vol. 12, no. 1s, pp. 443–456, Sep. 2023.
[19] J. Singh, S. Rani, and G. Srilakshmi, “Towards Explainable AI: Interpretable Models for Complex Decision-making,” 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), pp. 1–5, Apr. 2024.
[20] J. Singh, S. Rani, and P. Kumar, “Blockchain and Smart Contracts: Evolution, Challenges, and Future Directions,” 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), pp. 1–5, Apr. 2024.
[21] J. Singh, S. Rani, and S. Devi, “Comment on ‘Prediction of Metabolic Dysfunction–Associated Steatotic Liver Disease via Advanced Machine Learning Among Chinese Han Population,’” Obesity Surgery, Sep. 2025.
[22] J. Singh, S. Rani, and V. Kumar, “Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks,” International Journal of Communication Networks and Information Security (IJCNIS), Aug. 2024.
[23] J. Singh, S. Rani, S. Devi, and J. Kaur, “A Systematic Study on Recommendation System for E-Commerce Applications,” 2025 Seventh International Conference on Computational Intelligence and Communication Technologies (CCICT), pp. 221–226, Apr. 2025.
[24] K. V. Deshpande and J. Singh, “A Systematic Review on Website Phishing Attack Detection for Online Users,” International Journal of Image and Graphics, Jan. 2025.
[25] K. V. Deshpande and J. Singh, “Weighted transformer neural network for web attack detection using request URL,” Multimedia Tools and Applications, vol. 83, no. 15, pp. 43983–44007, Oct. 2023.
[26] P. Nasra et al., “Optimized ReXNet variants with spatial pyramid pooling, CoordAttention, and convolutional block attention module for money plant disease detection,” Discover Sustainability, vol. 6, no. 1, May 2025.
[27] R. K. K, P. M, J. Singh, G. Surendra, S. M. Ali, and M. R. B, “BlockStream Solutions: Enhancing Cloud Storage Efficiency and Transparency through Blockchain Technology,” International Journal of Electrical and Electronics Engineering, vol. 11, no. 7, pp. 134–147, Jul. 2024.
[28] S. Devi, O. Yadav, S. Rani, J. Singh, C. Dhavale, and S. Khanvilkar, “Blockchain Integration in Crowdfunding: A Smart Contract-Based Approach to Fundraising,” 2025 Seventh International Conference on Computational Intelligence andCommunication Technologies (CCICT), pp. 308–312, Apr. 2025.
[29] S. Jadhav and J. Singh, “Design of EGTBoost Classifier for Automated External Skin Defect Detection in Mango Fruit,” Multimedia Tools and Applications, vol. 83, no. 16, pp. 47049–47068, Oct. 2023.
[30] S. Jadhav-Mane and J. Singh, “Mango Skin Disease Detection Techniques Based on Machine Learning Techniques: A Review,” Wireless Personal Communications, vol. 139, no. 4, pp. 1881–1904, Dec. 2024.
[31] I. Ganie and S. Jagannathan, “Lifelong learning-based optimal trajectory tracking of constrained nonlinear affine systems using deep neural networks,” IEEE Trans. Cybern., pp. 1–14, 2024.
[32] I. Ganie and S. Jagannathan, “Lifelong reinforcement learning tracking control of nonlinear strict-feedback systems using multilayer neural networks with constraints,”

Neurocomputing, vol. 600, pp. 128–139, 2024.
[33] I. Ganie and S. Jagannathan, “Online Continual Reinforcement Learning-Based Optimal Output Tracking Control of Nonlinear Systems Using a Multilayer Observer,” Proc. 2025 Int. Joint Conf. Neural Netw. (IJCNN), Rome, Italy, 2025.
[34] T. Jagadeesan and T. Jesudas, "Selection of computer numerical controller parameters based on an adaptive control system by reducing environmental impact," Journal of Environmental Protection and Ecology, vol. 24, no. 4, pp. 1434–1439, 2023.
[35] T. Prabhu and T. Jesudas, "An efficient optimisation technique for minimising the environmental pollution and job shop scheduling challenges in real-time applications," Journal of Environmental Protection and Ecology, vol. 24, no. 5, pp. 1800–1805, 2023.
[36] T. Prabhakaran and T. Jesudas, "A novel cognitive intelligence network with architecture for trajectory recognition and prediction of destinations," Journal of Environmental Protection and Ecology, vol. 24, no. 5, pp. 1692–1700, 2023.
[37] B. Bindhu and T. Jesudas, "Application of Firefly and Flower Pollination Algorithm for wireless sensor network localization," Proceedings of the Bulgarian Academy of Sciences, vol. 76, no. 5, pp. 769–777, 2023.
[38] H. R. Laskar, “Adoption of fintech and digital financial services (DFS) by young professionals,” Int. J. Adv. Res. Eng. Technol., vol. 11, no. 1, pp. 537–561, 2020.
[39] H. R. Laskar, “Factors influencing saving and investment behavior of government and private sector employees,” Indian Journal of Economics and Business, vol. 20, no. 1, pp. 1168–1192, 2021.
[40] S. Roushon and H. R. Laskar, “Influence of Neural Behaviour on Decision Making,” IOSR Journal of Humanities and Social Science, vol. 29, no. 5, ser. 13, pp. 35–42, May 2024.
[41] Z. Alam and H. R. Laskar, “The Influence of Neural Behavior on Individuals’ Financial Decisions,” Journal of Economics, Finance and Management Studies, vol. 7, no. 6, pp. 3298–3306, Jun. 2024.
[42] S. Laskar, H. R. Laskar, and M. N. I. Barbhuyan, “Perception of Women Entrepreneurs Regarding Social Media Marketing,” Bangladesh Journal of Multidisciplinary Scientific Research, vol. 9, no. 5, pp. 10–18, Nov. 2024.
[43] S. Jadhav-Mane and J. Singh, “Mango Skin Disease Detection Techniques Based on Machine Learning Techniques: A Review,” Wireless Personal Communications, vol. 139, no. 4, pp. 1881–1904, Dec. 2024.
[44] S. Rani, J. Singh, and S. Devi, “Comment on ‘Evaluating Protein Liquid Supplementation for Enhanced Protein Intake and Adherence at Short-Term After Metabolic and Bariatric Surgery: A Pilot Randomized Controlled Trial,’” Obesity Surgery, Sep. 2025.
[45] S. Rani, J. Singh, and S. Devi, “Comment on ‘Oncologic and perioperative outcomes following robot-assisted radical prostatectomy in morbidly obese patients: a systematic review and meta-analysis,’” Journal of Robotic Surgery, vol. 19, no. 1, Sep. 2025.
[46] A. Dhanai, H. S. Bagde, R. Gera, K. Mukherjee, C. Ghildiyal, and H. Yadav, “Case report on irritational fibroma,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S960–S962, Feb. 2024.
[47] H. Bagde, A. Dhopte, F. Bukhary, N. Momenah, F. Akhter, O. Mahmoud, K. P. Shetty, M. A. Shayeb, H. Abutayyem, and M. K. Alam, “Monkeypox and oral lesions associated with its occurrence: a systematic review and meta-analysis,” F1000Research, vol. 12, p. 964, Mar. 2024.
[48] H. Bagde, R. S. Karki, S. Husain, S. Khan, V. Haripriya, and P. Purwar, “Evaluation of microbiological flora in endo-perio lesions before and after treatment,” Journal of Pharmacy and Bioallied Sciences, vol. 17, suppl. 2, pp. S1707–S1709, Jun. 2025.
[49] B. Shyamsukha, H. Bagde, A. Sharan, M. Choudhary, A. Duble, and A. V. Dhan, “Evaluating the potential of ChatGPT as a supplementary intelligent virtual assistant in periodontology,” Journal of Pharmacy and Bioallied Sciences, vol. 17, suppl. 2, pp. S1415–S1417, Jun. 2025.
[50] H. S. Bagde, M. K. Alam, A. K. A. Alhamwan, H. M. H. Aljubab, F. F. A. Alrashedi, D. H. M. Aljameeli, and M. G. Sghaireen, “The effect of a low-carbohydrate diet on periodontal

health and inflammation in patients with type 2 diabetes," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S641–S643, Feb. 2024.
[51] H. S. Bagde, M. K. Alam, Y. E. M. Almohammed, S. M. M. Almaqawid, A. W. N. Alanazi, F. T. F. Alanazi, and M. G. Sghaireen, "The efficacy of platelet-rich plasma as an adjunct to bone grafting in alveolar ridge preservation following tooth extraction," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S564–S566, Feb. 2024.
[52] S. B. Mangalekar, H. S. Bagde, M. Sale, S. V. Jambhekar, C. Patil, and C. V. Deshmukh, "Comparing laser-assisted and conventional excision in the management of oral soft lesions: a prospective clinical study," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S859–S861, Feb. 2024.
[53] M. K. Alam, H. S. Bagde, A. K. A. Alhamwan, H. M. H. Aljubab, F. F. A. Alrashedi, D. H. M. Aljameeli, and M. G. Sghaireen, "Comparing the long-term success rates of immediate implant placement vs delayed implant placement in patients with periodontally compromised teeth," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S626–S628, Feb. 2024.
[54] H. S. Bagde, M. K. Alam, Y. E. M. Almohammed, S. M. M. Almaqawid, K. K. Ganji, and M. G. Sghaireen, "Comparing the clinical and radiographic outcomes of two different surgical approaches for treating infrabony defects in chronic periodontitis patients," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S567–S569, Feb. 2024.
[55] A. Sharan, B. Pawar, H. Bagde, T. K. Chawla, A. V. Dhan, B. Shyamsukha, and S. Sharma, "Comparative evaluation of dentin hypersensitivity reduction over one month after a single topical application of three different materials: a prospective experimental study," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 4, pp. S3405–S3407, Dec. 2024.
[56] J. Prakash, T. Sinha, H. Bagde, N. Rajegowda, S. Bhat, A. Dhopte, M. Cicciù, and G. Minervini, "Evidence-based assessment of temporomandibular disorders in complete denture versus partial denture users: a systematic review," Minerva Dental and Oral Science, Sep. 2025.
[57] J. R. Rogers, Y. Wang, N. F. Khan, K. Mott, V. K. Nomula, D. Wang, P. C. Fiduccia, M. Burcu, and X. Liu, "Landscape assessment of clone-censor-weight methodology application in real-world data studies: A scoping review," in Proceedings of the Pharmacoepidemiology and Drug Safety Conference, vol. 33, pp. 424–424, Nov. 1, 2024.
[58] I. A. Mohammed, "Artificial Intelligence in Supplier Selection and Performance Monitoring: A Framework for Supply Chain Managers," Educational Administration: Theory and Practice, vol. 29, no. 3, pp. 1186–1198, 2023.
[59] I. A. Mohammed, "The Role of Artificial Intelligence in Enhancing Business Efficiency and Supply Chain Management," Journal of Information Systems Engineering and Management, vol. 10, no. 10s, pp. 509–518, Feb. 2025.
[60] I. A. Mohammed, "AI-Powered Risk Management Frameworks for Ensuring Supplier Quality in Carbon Capture and Energy Storage Supply Chains," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 1, pp. 854–, Dec. 2023.
[61] I. A. Mohammed, "Optimizing Carbon Capture Supply Chains with AI-Driven Supplier Quality Management and Predictive Analytics," Journal of Next-Generation Research 5.0, Dec. 2024.
[62] I. A. Mohammed, "Machine Learning-Driven Predictive Models for Enhancing Supplier Reliability in Renewable Energy Storage Supply Chains," International Journal of Intelligent Systems and Applications in Engineering, pp. 767–770, 2022.
[63] N. Gupta, M. Adawadkar, I. A. Mohammed, S. Verma, and M. Dubey, "Predictive Insights: Leveraging Artificial Intelligence for Strategic Business Decision-Making," Advances in Consumer Research, vol. 2, pp. 98–105, 2025.
[64] K. Chitra, S. S. Priscila, E. S. Soji, R. Rajpriya, B. Gayathri, and A. Chitra, "Transforming electrical simulation and management with smart grid technologies," International Journal of Engineering Systems Modelling and Simulation, vol. 16, no. 4, pp. 241–253, 2025.
[65] M. V. Soosaimariyan, H. L. Allasi, K. Chitra, and J. B. Gnanadurai, "Enhanced EMG-based hand gesture recognition by using generalized deep infomax networks," Journal of Sensors,

vol. 2025, no. 1, p. 9496890, 2025.
[66] K. Lakshmi and K. Chitra, “Stress Net: Multimodal stress detection using ECG and EEG signals,” Journal of Data Science, vol. 2024, no. 59, pp. 1–8, 2024.
[67] S. Rishabh, K. Chitra, and C. S. Yap, “A study on non-fungible tokens marketplace for secure management,” INTI Journal, vol. 2024, no. 18, pp. 1–8, 2024.
[68] S. Shreyash, S. Gaur, K. Chitra, and M. Y. N. Zuhaili, “EasyLearnify – A student study portal,” INTI Journal, vol. 2024, no. 17, pp. 1–6, 2024.
[69] S. K. R. Padur, “Engineering Resilient Datacenter Migrations: Automation, Governance, and Hybrid Cloud Strategies,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 2, no. 1, pp. 340–348, 2017.
[70] S. K. R. Padur, “From Centralized Control to Democratized Insights: Migrating Enterprise Reporting from IBM Cognos to Microsoft Power BI,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 6, no. 1, pp. 218–225, 2020.
[71] S. K. R. Padur, “Deep Learning and Process Mining for ERP Anomaly Detection: Toward Predictive and Self-Monitoring Enterprise Platforms,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 7, no. 5, pp. 240–246, 2021.
[72] S. K. R. Padur, “AI-Augmented Enterprise ERP Modernization: Zero-Downtime Strategies for Oracle E-Business Suite R12.2 and Beyond,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 9, no. 3, pp. 886–892, 2023.
[73] S. K. Somayajula, "Enterprise Data Migration Success Patterns: Lessons from Large-Scale Transformations," International Journal of Research in Computer Applications and Information Technology (IJRCAIT), vol. 8, no. 1, pp. 757-776, Jan.-Feb. 2025.
[74] S. K. Somayajula, "Demystifying Modern Data Warehousing: From Traditional to Cloud-Native Solutions," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025.
[75] S. K. Somayajula, "Building a Career in Enterprise Data Architecture: A Practical Guide," International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), vol. 7, no. 1, Jan. 2025.
[76] S. K. Somayajula, "Advanced ETL Optimization: A Framework for Next-Generation Data Integration," International Journal of Computer Engineering and Technology (IJCET), vol. 16, no. 1, pp. 381-406, Jan.-Feb. 2025.
[77] S. Somayajula and A. Orlovsky, "Proof, Truth and Contradiction in the System and Meta-System: Comprehensive Mathematical Solutions and Implementation Framework," 2025.
[78] P. Nutalapati, "Automated Incident Response Using AI in Cloud Security," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 2, no. 1, pp. 1301–1311, 2024
[79] P. Nutalapati, "Data Leakage Prevention Strategies in Cloud Computing," European Journal of Advances in Engineering and Technology, vol. 8, no. 9, pp. 118–123, 2025.
[80] P. Nutalapati, "Security Considerations for Hybrid Cloud Deployments in Fintech Using Blockchain," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 1, no. 1, URF Publishers, 2025.
[81] P. Nutalapati, "Zero Trust Architecture in Cloud-Based Fintech Applications," Journal of Artificial Intelligence & Cloud Computing, vol. 2, no. 1, pp. 1–8, 2023.
[82] P. Nutalapati, J. R. Vummadi, S. Dodda and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," 2025 International Conference on Data Science and Its Applications (ICoDSA), Jakarta, Indonesia, 2025.
[83] P. Nutalapati, S. M. Dhavale, A. Shrivastava, R. V. S. Praveen, H. K. Vemuri and R. RiadHwsein, "IoT and Machine Learning-Enhanced Energy Management in Enabled Smart Grids for Predictive Load Balancing," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025.
[84] P. Nutralapati, “Disaster Recovery and Business Continuity Planning in Cloud-Blockchain Infrastructures,” SSRN Electron. J., Jun. 2020.
[85] R. Boina, “Assessing the Increasing Rate of Parkinson’s Disease in the US and its Prevention

Techniques”,” International Journal of Biotechnology Research and Development, vol. 3, no. 1, pp. 1–18, 2022.
[86] P. M. Srinivas, K. Shivanna, D. R. Janardhana, and S. Samarth, “SAAI—Smart automated anti-violence intervention,” in Proc. 2024 Int. Conf. on Computing, Semiconductor, Mechatronics, Intelligent Systems and Communications (COSMIC), Nov. 2024, pp. 82–87.
[87] D. R. Janardhana, K. Shivanna, and A. P. Manu, “Security and privacy in military application using blockchain,” in Artificial Intelligence for Military Applications with Blockchain. Boca Raton, FL, USA: CRC Press, 2025, pp. 1–18.
[88] D. R. Janardhana, A. P. Manu, K. Shivanna, and K. C. Suhas, “Malware analysis and its mitigation tools,” in Malware Analysis and Intrusion Detection in Cyber-Physical Systems. Hershey, PA, USA: IGI Global, 2023, pp. 263–284.
[89] D. Ganesan, V. J. Francina, and V. P. Rameshkumaar, "Effectiveness of Corporate Responsibility Advertising Messages of Automobile Companies among Audience Perception," International Journal of Mechanical Engineering and Technology (IJMET), vol. 10, no. 2, pp. 934–941, 2019.
[90] K. Priya, R. V, S. A. Krishnan, V. P. Rameshkumaar, B. Premkumar and P. Jyothi, "Exploring Effective Leadership Strategies to Drive Organisational Success & Foster Sustainable Growth," 2024 Second International Conference on Advances in Information Technology (ICAIT), Chikkamagaluru, Karnataka, India, 2024.
[91] K. Priya, V. Rohini, S. A. Krishnan, V. P. Rameshkumaar, B. Premkumar, and P. Jyothi, "Exploring Effective Leadership Strategies to Drive Organisational Success & Foster Sustainable Growth," in Proc. 2024 Second International Conference on Advances in Information Technology (ICAIT), vol. 1, pp. 1–6, Jul. 24, 2024. IEEE.
[92] K. Selvavinayagam, V. J. Francina, and V. P. Rameshkumaar, "Evaluation of Logistic Performance Index of India in the Indian Postal Services," International Journal of Engineering and Management Research (IJEMR), vol. 8, no. 5, pp. 80–87, 2018.
[93] U. A. K. Yokubbaeva, P. P. Devi, S. Mahadevan, and D. S. U. Sharipov, "Words and algorithms: The intersection of linguistic and artificial intelligence," AIP Conf. Proc., vol. 3306, p. 050005, 2025.
[94] V. Devi Vanniarajan and S. Shfmkari, "Service quality of life insurance companies at Salem," Global Business Review, vol. 2, no. 2, pp. 23-31, 2008.
[95] V. Kumar, P. P. Devi, T. N. Babu, A. S. Nader, A. A. S. Mohammed and R. Saravanakumar, "AI-Powered Recruitment Marketing Enhancing Candidate Experience and Employer Branding," 2025 IEEE International Conference on Emerging Technologies and Applications (MPSec ICETA), Gwalior, India, 2025, pp. 1-6.
[96] P. Jothilingam, “Artificial intelligence applications for asset management systems: Enhancing reliability, optimization and decision-making in industrial environments,” International Journal of Business, Management and Visuals (IJBMV), vol. 4, no. 1, pp. 48–53, Jan. 2021.
[97] P. Jothilingam, “AI-Enabled Predictive Maintenance for Optimizing Plant Operations: Data-Driven Approaches for Fault Detection, Diagnostics, and Lifecycle Management,” International Journal of Open Publication and Exploration (IJOPE), vol. 8, no. 20, pp. 58–63, Jul. 2020.