
Journal of Informatics and Web Engineering

Vol. 4 No. 3 (October 2025)

eISSN: 2821-370X

Societies' Funds Management System Using Blockchain

**Jun Xiang Lau¹, Nur Ziadah Harun^{2*}, Suziyanti Marjudi³, Abd Samad Hasan Basari⁴,
Nur Amlya Abd Majid⁵, Roziyani Setik⁶**

^{1,2,3,4}Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Jalan Delta 1/6, Parit Raja, Batu Pahat, 86400, Malaysia.

⁵Tamhidi Centre, Universiti Sains Islam Malaysia, Bandar Baru Nilai 71800, Nilai, Negeri Sembilan, Malaysia.

⁶Faculty of Communication, Visual Art and Computing, Universiti Selangor, Jalan Timur Tambahan 45600 Bestari Jaya, Selangor, Malaysia.

*corresponding author: (nurziadah@uthm.edu.my; ORCID: 0000-0001-8045-7569)

Abstract - Lack of transparency of the funds and lack of immutability of the funds' records are large problems today, especially in the societies' funds. Leveraging the Ethereum Blockchain, the system ensures complete transparency and security in recording and accessing financial transactions for any society. Advanced encryption and blockchain consensus protocols guarantee data privacy and resilience against fraud or tampering. The information entered in the system helps the treasurer to effectively manage funds and accurately and transparently pass appropriate financial transactions. This project meets the challenges of transparency and immutability in society's fund records, providing an assurance system and promoting growth for the community's financial integrity. According to the iterative development model, the major components are user login, user management, payment status monitor, and funds history. A solution for a live transparent platform for their team members to have access to their financial data to build trust and get them involved. The system organizes the administrative tasks of bookkeeping, enabling the treasurer to be financially secure while maintaining trackable transactions. The key module of this system includes user login, user management, payment status tracking, and funds history. In the end, this project solves the stated problems by providing a safe path for growth and financial transparency.

Keywords— Funds Management, Blockchain, Transparency, Ethereum, Integrity, One Time Pad.

Received: 24 May 2025; Accepted: 26 August 2025; Published: 16 October 2025

This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



1. INTRODUCTION

The Societies Fund oversees all the pooled resources that have been entrusted to various societies. Such funds arise out of subscriptions paid by members, donations from outsiders, and revenues from any events organized by societies; usually, societies use this fund to offer some services or run initiatives. It is proper management, such as having a set budget and keeping track of expenses, as well as planning and documentation of finances. With the funds, major



Journal of Informatics and Web Engineering

<https://doi.org/10.33093/jiwe.2025.4.3.27>

© Universiti Telekom Sdn Bhd.

Published by MMU Press. URL: <https://journals.mmupress.com/jiwe>

activities can be arranged, projects that the top' societies work on can be undertaken, and services can be accessed. Effective management of these resources becomes vital in terms of financial stability and the transparency of societies.

Blockchain is a distributed and immutable ledger technology that facilitates the recording of transactions and the tracking of assets across a network. This digital ledger records cryptocurrency transactions in a chronological, public way so that at any given point in time, there is an open and unchangeable chain of blocks. One of the special characteristics of the blockchain is that it accomplishes decentralization without employing any central authority [1]. It forms a secure and transparent chain that eliminates the need for a central authority to ensure decentralization. For a cryptocurrency, they might involve ensuring that new transactions in a block were not fraudulent, or that coins had not been spent more than once [2]. Blockchain is mostly known for maintaining a secure and decentralized record of transactions as a part of cryptocurrency systems, but it does not limit itself to cryptocurrency uses.

Societies' funds often face critical challenges arising from limited transparency and the lack of immutable records. Lower transparency of the funds makes people not know what happened to the existing funds, such as the total amount of the funds and where the funds are used. Only the treasurer knows the information about the funds. While in the physical record, the fund's record is easy to manipulate. The members of society will be afraid that the funds in society will be abused or embezzled. This blockchain method overcomes the transparency record issues of the funds. Not just to reassure the members but to protect the treasurer. The treasure will simply not be misread when deploying blockchain ledgers to govern the wealth of a society. Using this model, the transparency of the funds and the immutability of the funds' records can be ensured because everyone can view the information about the funds, and the records cannot be altered. This is what makes the funds more secure and transparent. Then the treasurer of the society can manage the society's funds easily through the system.

To address these challenges, blockchain technology is being proposed as a solution for society's capital management systems. This is the most common a treasurer, which is conducting efficient recording of data and transactions, and a basis method of keeping track of any society's funds. This process can be very tedious and lengthy. Now, due to this amazing technology called Blockchain, this process would take much less time for data management [3]. The Society Funds Management System is a platform that intends to improve the management of society funds using blockchain technology. It helps to not only use blockchain technology to enhance the transparency and security of financial transactions but also to bring in an immutable record of any data entered and not altered or deleted. This way, there would always be a permanent history of all transactions. Operations could also be made more efficient and faster by the capacities of the blockchain, thereby serving as a vital tool for the modern fund management system.

2. LITERATURE REVIEW

This section provides a comprehensive literature review conducted for this project, including several critical aspects of the proposed Societies' Funds Management System. This explores the concept of decentralization, emphasizing its important role in distributing decision-making and operational responsibilities, focuses specifically on Ethereum as a blockchain-based software platform.

2.1 Societies' Funds Management System

Developing a blockchain-based funds management system requires a critical framework, as the management of social finances is a matter of utmost importance. Contributions from members, donations from benefactors, and proceeds from events or activities, the funds are administered. By insisting on growth and improvement along with the society's well-being of its members, such funds represent the society's right to claim autonomy over itself [4]. Fundraising comes from many avenues, and the funds are recorded and managed by the treasurer. But it is very opaque because the members cannot easily view real-time information about how much money is in the system and how it is being applied. In the process, there could be fears about possible misuse or misappropriation. Problems with immutability arose because if it was on paper, it could be altered, and thus, people were distrustful that the financial information was accurate. The blockchain solution seeks to provide greater transparency by allowing all members to see the fund information, immutability through the distributed nature of cryptocurrency blockchain, maintaining good records for the treasurer, and effectively managing funds through a secure platform.

2.2. Decentralization System

Decentralized systems are those in which central entities play a lesser role in any or all of these dimensions [5]. This means that the database does not depend on a specific organization or administrator but is distributed among all peers [6]. In a decentralized system, decision-making and operational responsibilities are dispersed among multiple individuals, nodes, or entities rather than being concentrated in a central governing body. This distribution of power aims to promote greater autonomy, transparency, and resilience within a network or organization [7]. Decentralization can be applied across various domains, including governance, technology, finance, and information systems. In the context of technology and blockchain, decentralization often refers to the absence of a central authority or intermediary in a network. Instead, data and control are distributed across a network of nodes, and decisions are made through consensus mechanisms. This design enhances security, reduces the risk of a single point of failure, and fosters trust among participants. Decentralized systems are often contrasted with centralized systems, where control and decision-making are concentrated in a single, central entity. Centralized refers to the contractual relationship between an "agent" and a "principal." It deals with the delegation of authority from the principal to the agent to act on their behalf [8]. The concept of decentralization has gained prominence in various fields to promote efficiency, transparency, and resilience in the face of potential centralization-related drawbacks.

2.3. Blockchain

Blockchain is popularly viewed as a ledger recording all transactions that occur between peers on the network [9]. In a blockchain, a series of transactions that are placed together into blocks, where each block is linked to its immediate predecessors, creating an immutable chain [10]. The main innovation here is decentralization, in which there is no central authority, and each participant in the network holds a complete copy of the ledger so that agreement may take place on transaction validity, whereas security of the data would be obtained by cryptographic techniques such as hashing and digital signatures. After being added to the blockchain, a block becomes unmodifiable and offers a tamper-proof record of transactions. Figure 1 illustrates how the blockchain works in that a transaction, which in essence may capture the value transfer between two entities, is originally packed into a box and the box is subsequently broadcast to the members of the network for validation. This validation ensures the validity and integrity of transactions, preventing tampering. Once validated, the block is appended to the blockchain, a public ledger of all transactions. Finally, the updated ledger is distributed across the network, maintaining consistency among all participants.

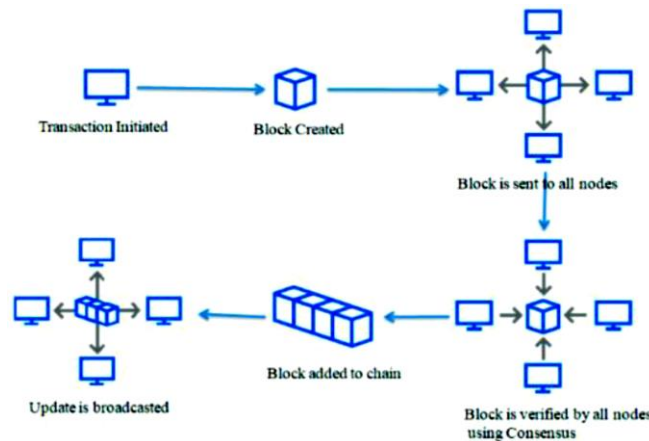


Figure 1. The operation of a Blockchain [11]

Ethereum is a specific blockchain-based software platform that enables the possibility of building and running smart contracts and the so-called Distributed Applications (DApps) [12]. The block header of the Ethereum blockchain consists of several components, which are the Keccak 256-bit hash of the parent block's header, the address of the recipient who receives the mining fee, hashes of state, transaction, and receipts tries, the difficulty, the current gas limit of the block, a number representing the total gas used in the block's transactions, timestamp, nonce, and other hashes for verification purpose[13]. Ethereum's key distinguishing factor from Bitcoin is that it offers an entire standard programmable platform that developers can use to deploy smart contracts. Ether (ETH), the internal cryptocurrency of Ethereum, facilitates transactions with other parties in the network and compensates them. Ethereum

is going to be utilizing a decentralized network to validate transactions on the new Proof of Stake (PoS), a transition from a previous Proof of Work. The framework permits the development of different applications, from decentralized financial (DeFi) protocols to non-fungible tokens (NFTs), which helps enhance creativity and adds a remarkably significant touch to the wide ecosystem of blockchain.

2.4. Security Features

Apart from blockchain technology, there are some additional security features that are used in this project, which are hashing, two-factor authentication (2FA), and encryption.

2.4.1. Hashing

The hash function maps an arbitrary-length data unit into a fixed-length value, also known as the hash value or hash code [14]. This fixed-length value becomes a unique fingerprint for the original data and is used for multiple purposes, such as data integrity, data security, and data indexing. Hashing is therefore a one-way function wherein calculating the hash from the data is easy, but reversing the process to derive the underlying data from the hash is computationally impractical [15]. This essentially helps keep the data secure since the attackers will find it impossible to steal or modify information without being caught. Furthermore, hash functions exhibit collision resistance, which means that it should be difficult to get two different inputs that map to the same hash value. These characteristics greatly assist in the secure and efficient hashing work. Hashing has many applications, from digital signatures and password storage, through file checksums to blockchain technology.

2.4.2. 2FA

2FA is a way to protect the account by making sure you are who you say you are by giving two different pieces of information. These factors usually fit into one of three groups: something you know, something you have, or something you are [16]. 2FA is a common way to make email accounts, banking websites, and social media platforms safer. It adds another layer of protection against unauthorized access, especially when passwords alone may be easy to steal or hack. Having more than one factor makes it harder for attackers to get into an account because they would need both the user's password and access to their second factor.

2.5. Comparison Between Existing Systems and Proposed Systems

The comparison is based on different features of a societies' funds management system that needed to be effective and trusted. Table 1 shows the comparison between existing systems and the proposed system.

Table 1. Comparison of Existing Systems

Feature	iSocietyManager [17]	SocietyPlus [18]	Proposed System
System based	Cloud-based	Cloud-based	Blockchain-based
Data Transparency	Yes	Yes	Yes
Data immutability	No	No	Yes
2FA	Yes	Yes	Yes

According to Table 1, the current systems are based on the cloud, while the new system is based on blockchain. The three systems all have similar features, like making data clear, requiring 2FA, and encrypting data. However, the proposed system is different from the other two because it offers data immutability. This means that once information is put on the blockchain, it can't be changed or deleted. This is a useful part of the societies' funds management system because it can help stop fraud and corruption. In general, the proposed system looks like a good new way to handle the money of societies. It has all the features of the other two systems, plus the extra security of data that can't be changed.

Currently, fund management systems suffer from several major shortcomings. The process for manually uploading and validating transaction slips is time-consuming, cumbersome, and error-prone, whereas having the trustless characteristics of blockchain embedded with IPFS will ensure the validity and automation of manual uploads. When only the treasurer has control of the records of the funds managed by society, there is limited transparency on how funds are disbursed. On-chain storage utilizes an immutable but visible record on the blockchain that can be seen by all members, which preserves the transparency and integrity of funds within one's control. On the other hand, IPFS hashes recorded onto the blockchain are much more secure against manipulation than conventional physical or centralized records, and any digital record of any version can be traced to detect any type of tampering [19]. The proposed blockchain-based approach also contributes to a more complete audit trail, compared with conventional fund management systems that offer no assurance of full disclosure or transparency. In having a permanent log of verifiable records of every step taken, blockchain effectively fills in gaps in existing fund management solutions [20]. By working with proven blockchain concepts, in conjunction with utilizing a decentralized storage method and a simple interface, the proposed system provides significant solutions to eliminate usability and technical gaps in existing fund management solutions [21]. Therefore, the proposed system addresses gaps in existing fund management approaches by introducing automated verification through IPFS, ensuring transparency [22] with immutable on-chain records, and providing auditability and usability features that current systems often lack [23].

3. SYSTEM DESIGN

This section presents the system design in a simple form that can be easily understood by users when they see the diagram. Firstly, the user makes a transaction then when the transaction is successful, the user needs to upload the slip of transaction. The slip will be embedded into the blockchain to ensure the data cannot be manipulated. Users are allowed to view the record or history of transactions they make. Figure 2 shows the system architecture diagram.

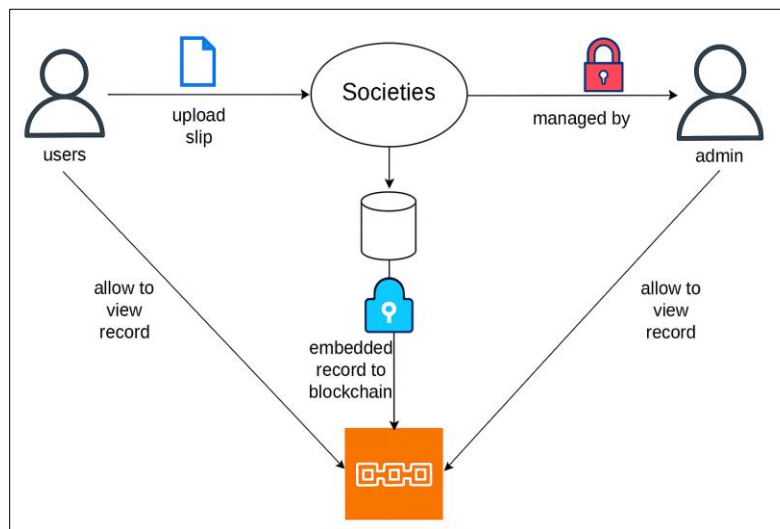


Figure 2. System Architecture Diagram

4. IMPLEMENTATION

This section discusses the implementation of Societies' Funds Management System. There are three implementations that will be discussed, which are the implementation of security modules, the blockchain environment, and system properties.

4.1 Implementation of Security Modules

The first security module is a safe login message. The system will not show which credential information is incorrect when the user enters the wrong login information. The system just displays the error message of "Invalid username or password," whether it is an incorrect username or password. Figure 3 shows an example of a failed login.

The screenshot shows a web form titled "Society's Funds Management System" with a "Login" section. It contains two input fields: "Username:" and "Password:". Below the fields is a green "Login" button, a link for "Forgot password?", and a red error message: "Invalid username or password!". At the bottom, there is a link for "Don't have an account? Register here."

Figure 3. Error Message When Login Failed

Secondly, the system requires a minimum length of the created password to comply with strong password authentication, which is at least 8 characters, and the password must include at least one upper- and lower-case alphabet, a numeric, and a special character. Algorithm 1 shows the implementation of a strong password.

Algorithm 1: Algorithm for ValidatePassword

Input: password (string)

Output: Boolean (true if valid, false if invalid)

1. **BEGIN**
 2. **DEFINE** validation pattern requiring:
 - a. At least one lowercase letter ($?=.*[a-z]$)
 - b. At least one uppercase letter ($?=.*[A-Z]$)
 - c. At least one digit ($?=.*\d$)
 - d. At least one special character from $[@!\%*?&]$
 - e. Minimum 8 characters length $\{8,\}$
 3. **TEST** password against pattern
 4. **IF** test **FAILS THEN**
 5. **SHOW** alert with requirements:
 - Minimum 8 characters
 - Needs uppercase
 - Needs lowercase
 - Needs digit
 - Needs special character
 6. **RETURN** false
 7. **END IF**
 8. **RETURN** true
 9. **END**
-

Thirdly, the destroy session is used to destroy the current session after the user clicks the logout button on the system. After the session is destroyed, the system will redirect the user to the login page. So that the user cannot use the system without logging in. Algorithm 2 shows the destroy session code.

Algorithm 2: Algorithm for LogoutUser

Input: None (uses existing session)

Output: Redirects to homepage

1. **BEGIN**
 2. **START** session handling
 3. **CLEAR** all session variables ($session_unset$)
 4. **DESTROY** the session ($session_destroy$)
-

-
5. **REDIRECT** user to *index.php*
 6. **TERMINATE** script execution (*exit*)
 7. **END**
-

Fourth, the system implements password hashing before the password is stored in the database. Password hashing is used to protect passwords from being seen directly from the database by others. Algorithm 3 shows the implementation of the password hashing.

Algorithm 3: Algorithm for HashPassword

Input: password

Output: hashed_password

1. **BEGIN**
 2. *hashed_password* \leftarrow *SecureHashFunction(password, DefaultAlgorithm)*
 3. *Return hashed_password*
 4. **END**
-

Lastly, the OTP is implemented in the registration process to verify the user's email. Users need to use a valid email to register for an account. Algorithm 4 shows the algorithm for the implementation of OTP. Through this project, OTP records, session tokens, and password authentication do not have any on-chain aspects, as they belong to the off-chain security and authentication layer. Blockchain technology supports ledger-based on-chain storage and references recorded as digital ownership.

Algorithm 4: Algorithm for Generate and Store OTP

Input: username, email, hashed_password

Output: OTP value stored in session and database

1. **BEGIN**
 2. **GENERATE** random 6-digit OTP between 100000-999999
 3. **SET** *expiryTime* = *current time* + 1 minute
 - 4.
 5. **STORE** in session:
 6. - *otp* = generated OTP
 7. - *username* = input username
 8. - *email* = input email
 9. - *password* = input hashed_password
 - 10.
 11. **PREPARE** database statement:
 12. **INSERT INTO** *otps*:
 13. - *username*
 14. - *email*
 15. - *otp*
 16. - *created_at* (*current time*)
 17. - *expires_at* (*expiryTime*)
 - 18.
 19. **EXECUTE** database statement
 20. **END**
-

4.2 Implementation of Blockchain Environment

Firstly, Metamask setup using Ganache. Metamask is a cryptocurrency wallet that is used to interact with the Ethereum Blockchain. Ganache provides a testing purpose use account to simulate the interaction between Metamask and the Ethereum Blockchain. Figure 8 shows the Metamask setup.

The second is ipfs gateway. The IPFS gateway is used to store the slip that the user uploads to the system. The IPFS gateway used in the system is Pinata. Figure 9 shows the interface of the Pinata IPFS gateway.

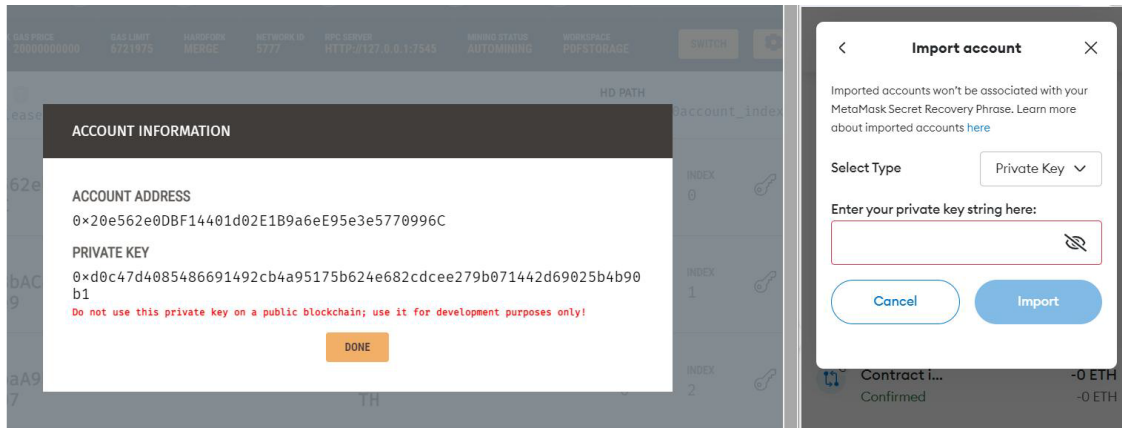


Figure 8. Metamask Setup

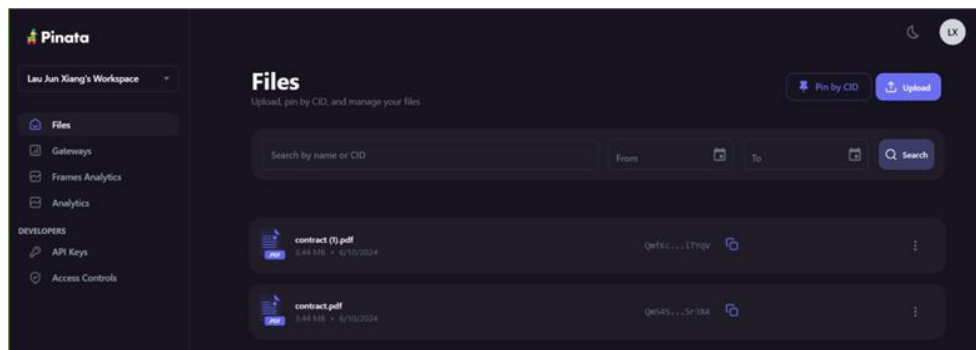


Figure 9. Pinata IPFS Gateway

The third is to upload and store it in the blockchain. When the user uploads their slip, they will get the IPFS hash of their slip. Then, the IPFS hash will be stored in the blockchain. Algorithm 5 shows the source code for uploading and storing to the blockchain. This section explains how the smart contract fits into the whole upload process, what it does, and why it matters.

The Society's Funds Management System uses a smart contract as a vital part of the immutability, transparency, and accountability of the document management system. The PDFs are not stored on-chain, but externally on the IPFS. The smart contract saves the metadata for the file on-chain, so that it can record the file references in a way that cannot be modified. The core logic exists in the `uploadFile()` method as shown in Algorithm 5, which needs two inputs from the user: `ipfsHash`, which is a unique identifier created by IPFS for the document, and the `fileName`. The uploader's (`msg.sender`) address is recorded implicitly. After the user calls the `uploadFile()` method using the bookkeeper smart contract, the Ethereum blockchain will take care of recording the document transaction, but the `uploadFile()` method first validates both inputs, creates a metadata object with a hash, filename, and a timestamp, and pushes this metadata record through a mapping for the uploader's account. In order to work with the off-chain applications involved, the contract will emit a `FileUploaded` event, with the uploader address, the hash for the file, the filename, and the time also for the timestamp. This allows the front-end applications to confirm the upload is complete and ensure they update their local records accordingly. The outputs from the `uploadFile()` function will be the on-chain blockchain transaction hash, the emitted event log as well as the immutable. On-chain record can be independently verified by a blockchain explorer. Then, users' data is secured by using IPFS to facilitate storage interaction in a decentralized format, and the smart contract employs the Ethereum blockchain for tamper-proof recording, which ensures data immutability and traceability of documents through an electronically enforceable recording procedure.

Figure 11 shows the verification of the uploaded slip. It is used to verify whether the uploaded slip is true or not.

Algorithm 5: Algorithm for Upload PDF**Input:** pdf file, pdfname, account**Output:** Success/Failure status

```

1. BEGIN
2. IF pdf is empty THEN
3.   RETURN
4. END IF
5.
6. TRY:
7. // Step 1: Package file
8.   Create formData
9.   Add pdf to formData
10.
11. // Step 2: Upload to IPFS
12.   Send POST to Pinata API with:
13.   - Headers: API keys
14.   - Body: formData
15.   Extract ipfsHash from response
16.
17. // Step 3: Record on blockchain
18.   Call smart contract's uploadFile:
19.   - Parameters: ipfsHash, pdfname
20.   - From: account
21.   Get transactionHash from response
22.
23. // Step 4: Store in local DB
24.   Send POST to local server with:
25.   - transaction_hash
26.   - ipfs_hash
27.   - file_name
28.
29. // Step 5: Update UI
30.   Add record to uploadHistory with:
31.   - txHash
32.   - ipfsHash
33.   - filename
34.   - status: success
35.
36. CATCH error:
37.   Add failure record to uploadHistory
38.   Log error
39. END TRY
40. END

```

Uploaded Slip

File Name	IPFS Hash	Status	Actions
contract (1).pdf	QmfKcgYRkErF3NubzS9JePTIZhZgq7hUYxQyDoodWITYqV		<input type="button" value="Verify"/> <input type="button" value="Reject"/>

Figure 11. Interface of Verification

5. CONCLUSION

The Societies' Funds Management System powered by blockchain technology offers several advantages such as offering immutable records of transactions; storing of encrypted user passwords utilizing hashing before storing in the database; and enforcing strong password requirements for user security. These characteristics improve data integrity and security, which are two foundations in financial management systems. At the moment, the user is required to upload transaction slips, and administrators are required to perform manual verification of slips, which is inefficient and delays the process.

There are several ways to improve the user experience for the system and to help scale it over time. At this moment, the blockchain implementation is using Ganache Testnet for testing, which is appropriate for a prototype, but does not have the resilience of a production implementation. Moving to the Ethereum platform, or a dedicated private blockchain in production mode, would make the system stronger, more reliable, and legitimate in terms of real-world uses. The adoption of banking APIs in the system could also eliminate users having to manually upload the transaction slips for their transactions and allow for more automatic verification of the transactions. This would reduce the amount of effort for the user and administrator in completing the user experience. Future research could also offer evidence on the adoption of smart contracts for the automatic disbursement of funds and auditing of transactions, and consensus mechanisms that would be more suited to an organizational financial system. In conclusion, the current system addresses some of the key issues of checking transparency and security.

ACKNOWLEDGEMENT

This research was supported by Universiti Tun Hussein Onn Malaysia (UTHM) through Tier 1 (vot J122). The authors would like to express their gratitude to unknown reviewers for the thoughtful review of this paper.

FUNDING STATEMENT

This research was supported by UTHM through Tier 1 (vot J122).

AUTHOR CONTRIBUTIONS

Jun Xiang Lau: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation;
Nur Ziadah Harun: Project Administration, Writing – Review, Editing & Approval;
Suziyanti Marjudi: Project Administration, Supervision, Writing – Review & Editing;
Abd Samad Hasan Basari: Project Administration, Supervision, Writing – Review & Editing;
Nur Amlyia Abd Majid: Project Administration, Writing – Review, Editing & Approval;
Roziyani Setik: Project Administration, Writing – Review, Editing & Approval.

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

The paper follows The Committee of Publication Ethics (COPE) guideline. <https://publicationethics.org/>.





REFERENCES



- [1] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of Blockchain technology: pros, cons and SWOT," *Cluster Computing*, vol. 22, no. 6, pp. 14743–14757, 2019, doi: 10.1007/s10586-018-2387-5.

- [2] N. Moosavi, H. Taherdoost, N. Mohamed, M. Madanchian, Y. Farhaoui, and I. U. Khan, "Blockchain technology, structure, and applications: A survey," *Procedia Computer Science*, vol. 237, pp. 645–658, 2024, doi: 10.1016/j.procs.2024.05.150.
- [3] D. Afrianita, "Village fund management in improving community welfare in socio-economic sector", *International Journal on Social Science, Economics and Art*, 9(3), pp. 128–142, 2019, doi: 10.35335/ijosea.v9i3.34.
- [4] A. Schneider, "Decentralization: Conceptualization and measurement," *Studies in Comparative International Development*, vol. 38, no. 3, pp. 32–56, 2003, doi: 10.1007/BF02686198.
- [5] L. Liu, S. Zhou, H. Huang, and Z. Zheng, "From technology to society: An overview of blockchain-Based DAO," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 204–215, 2021, doi: 10.1109/OJCS.2021.3072661.
- [6] N. McGinn, "Decentralization of education: why, when, what and how?," *UNESCO*, 1999. [Online]. Available: <https://www.researchgate.net/publication/44824547>
- [7] M. Pacheco, G. A. Oliva, G. K. Rajbahadur, and A. E. Hassan, "What makes Ethereum blockchain transactions be processed fast or slow? An empirical study," *Empirical Software Engineering*, vol. 28, no. 2, Mar. 2023, doi: 10.1007/s10664-022-10283-7.
- [8] K. Wust, and A. Gervais, "Do you need a blockchain?," in *Proceedings of the 1st Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, pp. 45–54, Jun. 2018, doi: 10.1109/CVCBT.2018.00011.
- [9] D. Guru, P. Supraja, & V. Vijayakumar, "Approaches towards blockchain innovation: a survey and future directions", *Electronics*, vol. 10, no. 10, pp. 1219, 2021, doi: 10.3390/electronics10101219.
- [10] K. Wust, and A. Gervais, "Do you need a blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, pp. 45–54, 2018, doi: 10.1109/CVCBT.2018.00011.
- [11] D. Guru, S. Perumal, and V. Varadarajan, "Approaches towards Blockchain Innovation: A Survey and Future Directions," *Electronics*, vol. 10, no. 10, pp. 1219, 2021, doi: 10.3390/electronics10101219.
- [12] S. Ferretti and G. D'Angelo, "On the ethereum blockchain structure: a complex networks theory perspective", *Concurrency and Computation: Practice and Experience*, vol. 32, no. 12, 2019, doi: 10.1002/cpe.5493.
- [13] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and Ethereum: a brief overview", *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1-6, 2018, doi: 10.1109/infotech.2018.8345547.
- [14] J. P. Conley, "Encryption, hashing, PPK, and blockchain: A simple introduction," 2019. [Online]. Available: <http://jpconley.wordpress.com/>
- [15] M. Winkler, C. Peither, S. Petrick, L. Seidemann, H. Jelich, F. Kleine Jager, J. Muller-Quade, A. Colsmann, H. Nirschl, and F. Rhein, "Physical one-way functions for decentralized consensus via proof of physical work," *Advanced Science*, vol. 12, no. 28, pp. 2409386, 2025, doi: 10.1002/advs.202409386.
- [16] E. Cristofaro, H. Du, J. Freudiger, and G. Norcie, "A comparative usability study of two-factor authentication", *Proceedings 2014 Workshop on Usable Security*, 2014, doi: 10.14722/usec.2014.23025.
- [17] iSocietyManager, "Enterprise facility management system," [Online]. Available: <https://isocietymanager.com/> (accessed: Jul. 2, 2025).
- [18] Society Plus, "Society plus - Creating smart societies | Since 1989," [Online]. Available: <https://www.societyplus.co.in/> (accessed: Jul. 2, 2025).
- [19] R. Almadadha, "Blockchain technology in financial accounting: Enhancing transparency, security, and ESG reporting," *Blockchains*, vol. 2, no. 3, pp. 312–333, 2024, doi: 10.3390/blockchains2030015.

- [20] L. Zhou, "Blockchain in finance: enhancing transparency and security in cross-border transactions", *Journal of Applied Economics and Policy Studies*, vol. 17, no. 1, pp. 56-60, 2025, doi: 10.54254/2977-5701/2025.21075.
- [21] M. Bhandari, G. Tiwari, and M. Dhakal, "Enhancing transparency and accountability in sustainable finance through blockchain technology: A systematic review of the literature", *Journal of Intelligent Management Decision*, vol. 4, no. 1, pp. 23-43, 2025, doi: 10.56578/jimd040102.
- [22] M. H. Z. . Hairul Nizam, M. A. . Ahmad Nizam, M. H. Husaini Jummadi, N. N. M. S. . Nik Mohd Kamal, and A. A. Zainuddin, "Hyperledger fabric blockchain for securing the edge Internet of Things: A review", *Journal of Informatics and Web Engineering*, vol.4, no.1, pp. 81–98, 2025, doi: 10.33093/jiwe.2025.4.1.7.
- [23] F. Mazlan, N. F. . Omar, N. N. M. S. . Nik Mohd Kamal, and A. A. Zainuddin, "Comprehensive Insights into Smart Contracts: Architecture, Sectoral Applications, Security Analysis, and Legal Frameworks", *Journal of Informatics and Web Engineering*, vol. 4, no. 1, pp. 1–17, Feb. 2025, doi: 10.33093/jiwe.2025.4.1.1.

BIOGRAPHIES OF AUTHORS

	<p>Jun Xiang Lau is a student in Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia. He has background in the Information Security and Cybersecurity. He can be contacted at email: jxlau10@gmail.com.</p>
	<p>Nur Ziadah Harun received the B.S. and M.Sc. degrees in Information Technology from Universiti Utara Malaysia, in 2008 and 2012, respectively, and the Ph.D. degree in Computer Network from Universiti Putra Malaysia. She has been a lecturer with the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, since 2020. Her research interests focus on quantum cryptography and network security. She is a member of the IEEE Computer Society. She can be contacted at email: nurziadah@uthm.edu.my.</p>
	<p>Suziyanti Marjudi is a Senior Lecturer at the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM). Her research focuses on artificial intelligence, data science, and big data analytics, with strong contributions in academic supervision, scholarly publications, and community engagement. She is passionate about bridging research with practical applications, particularly in education and industry collaboration. She can be contacted at email: suziyanti@uthm.edu.my.</p>
	<p>Abd Samad Hasan Basari is a professor at the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia. He obtained his B.Sc. (Hons.) in Mathematics from Universiti Kebangsaan Malaysia in 1998. In 2009, he obtained a PhD in Information and Communication Technology from Universiti Teknikal Malaysia Melaka, Malaysia. Professor Abd Samad is currently the Head of the Artificial Intelligence and Data Mining Research Centre (SMC), UTHM. He can be contacted at email: abdsamad@uthm.edu.my.</p>

	<p>Nur Amlia Abd Majid is a Lecturer at the Tamhidi Centre, Universiti Sains Islam Malaysia (USIM). She holds a Ph.D. in Industrial Computing from Universiti Kebangsaan Malaysia (2022), with research on supply chain disruption models in the livestock industry. Her work focuses on IoT and digital solutions for livestock management, particularly supplier profiling for animal feed. She is also active in curriculum development and applied research. She can be contacted at email: amlya@usim.edu.my.</p>
	<p>Roziyani Setik has served as a lecturer at the Faculty of Communication, Visual Art and Computing, Universiti Selangor, since 2007. She obtained her Master of Science in Information Management from Universiti Teknologi MARA, Shah Alam, and holds a Bachelor of Computer Science from Universiti Putra Malaysia. Her academic interests encompass big data, data mining, and data processing, with a particular emphasis on sentiment analysis of social media content related to specific topics. She can be contacted at email: roziyani@unisel.edu.my.</p>