Educational Administration: Theory and Practice
2024,30(5) 15048 - 15056
ISSN:2148-2403
https://kuey.net/

Research Article

Enhancing Financial Transaction Security With Blockchain Technology

Aakansha Mitawa[1*], Dr. Pawan Bhambu[2]

[1*]Computer Science & Engineering, Vivekananda Global University, Jaipur, Rajasthan, India.aakanshamitawa4694@gmail.com
[2]Computer Science & Engineering, Vivekananda Global University, Jaipur, Rajasthan, India. pawan.bhambu@vgu.ac.in

Citation: Aakansha Mitawa, et.al (2024), Enhancing Financial Transaction Security With Blockchain Technology, *Educational Administration: Theory and Practice, 30(5), 15048 - 15056*
Doi: 10.53555/kuey.v30i5.7508

ARTICLE INFO

ABSTRACT

Background: Cryptocurrency represents a modern digital payment system that operates independently of traditional banking institutions. Instead of physical currency, cryptocurrencies exist as digital entries within a virtual ledger, facilitating transactions globally without geographical constraints. The emergence of cryptocurrency has revolutionized how transactions are conducted, with a growing number of businesses—over 2,300 in the US alone—accepting Bitcoin and other digital assets for various purposes, including investments and operational transactions. This shift underscores the potential of cryptocurrencies and blockchain technology to reshape financial and operational practices across sectors.

Methodology: This research explores the integration of blockchain technology and cryptographic techniques in enhancing digital transaction security and operational efficiency. Specifically, we investigate the application of blockchain in sectors such as real estate, where it has been used to develop smarter contracts. Our study employs cryptographic hash functions to protect sensitive information. BLAKE2b-512 is utilized for hashing user identities, providing robust security due to its resistance to reverse engineering. Additionally, MD5 is used for hashing passwords, ensuring that even in the event of a database breach, user credentials remain secure.

Findings: The adoption of blockchain and cryptographic hashing techniques has shown significant improvements in transaction security and data protection. By storing hashed values instead of plaintext information, the risk of sensitive data being compromised is substantially reduced. Our findings highlight that while BLAKE2b-512 offers strong protection for user identities, the use of MD5 for password hashing presents a layered approach to safeguarding sensitive information. The study demonstrates that integrating these technologies not only enhances security but also fosters trust and efficiency in digital transactions and business operations.

Keywords: Blockchain, Security, bitcoin, cryptocurrency.

1 Introduction

Cryptocurrency represents a groundbreaking shift in the financial world, enabling digital transactions without the need for traditional banking systems. Leveraging cryptographic techniques, cryptocurrencies ensure secure and anonymous transactions through a decentralized framework. Unlike conventional currencies, cryptocurrencies operate within digital environments, recorded in virtual databases and managed through digital wallets. This system provides a level of security and anonymity derived from advanced cryptographic methods and the absence of central authorities [1].

The adoption of cryptocurrencies has surged, with numerous businesses embracing digital currencies for various purposes, including investment, operations, and transactions. This rapid integration into mainstream financial activities presents both significant opportunities and challenges. Companies entering the cryptocurrency space must carefully consider their objectives and strategies to navigate the complexities of this evolving market [2].

Cryptocurrencies, such as Bitcoin, Ethereum, and Litecoin, utilize blockchain technology to ensure decentralization, transparency, and immutability [3][4][5]. The blockchain functions as a distributed ledger that organizes data into blocks, which are then linked to form a continuous and secure chain. This structure is pivotal for maintaining transaction integrity and security, eliminating the need for intermediaries and reducing transaction fees [6][7]. However, the lack of a direct association between user identities and their cryptocurrency transactions remains a significant concern.

Our research addresses this gap by proposing a novel solution to link user identities with cryptocurrency transactions through the creation of a Digital Code Identity. By enhancing the existing blockchain framework with advanced cryptographic techniques, we aim to provide a more secure and traceable system for digital transactions. This approach is designed to meet the growing demands for enhanced security and efficiency in the cryptocurrency domain.

Objectives of Research

1. **Identify and Analyze Existing Problems:**
   - **Evaluate Framework Limitations:** Investigate the limitations and security gaps within the current cryptocurrency frameworks, particularly focusing on the absence of direct linkage between user identities and their transactions.
   - **Assess Security Risks:** Examine potential vulnerabilities and risks associated with the pseudonymous nature of cryptocurrency transactions, including issues related to fraud, theft, and regulatory compliance [8].
2. **Develop a Methodology for Enhanced Security:**
   - **Implement Advanced Cryptographic Techniques:** Utilize BLAKE2b, a high-speed cryptographic hash function, in conjunction with MD5 to create a secure Digital Code for Currency. This combination aims to enhance transaction processing speed and security.
   - **Create a Digital Code Identity:** Design a methodology to generate a unique Digital Code that links each cryptocurrency transaction to the user's identity. This system will improve transaction traceability and security.
3. **Propose a Cryptocurrency Model:**
   - **Design an Integrated Model:** Develop a cryptocurrency model that establishes a direct connection between digital currency and user identity through the Digital Code. This model seeks to enhance the traceability and integrity of transactions within the cryptocurrency network.
   - **Evaluate and Test the Model:** Conduct comprehensive testing to assess the effectiveness of the proposed model in improving security and transaction tracking. Evaluate the model's performance and its potential impact on the cryptocurrency ecosystem.

By addressing these objectives, our research aims to contribute significantly to the field of cryptocurrency, enhancing security and transparency in digital transactions while fostering greater trust and efficiency in the cryptocurrency market.

2 Literature Review

Takahashi and Lakhani (2019) focus on the increasing use of cryptocurrencies and the challenges of maintaining security in online transactions. They propose a method for conducting multiple-layered security analyses, particularly for cryptocurrency exchange services [13].

Sai et al. (2019) examine the security profiles of commonly used Android cryptocurrency applications. They compare their findings to control tests across cryptocurrency wallets, evaluating both security and privacy features. Despite limited functionality, traditional financial services apps are only marginally better in security but provide greater privacy measures [14].

Azman and Sharma (2020) discuss the transformative potential of Bitcoin in the global economy and present HCH DEX as a unique way to securely store cryptocurrency with a smart card setup for two-way authentication. The system aims to resist fraudulent and unethical policies, offering a step towards an economically fair environment [15].

Karanjai et al. (2021) introduce the design and implementation of a conditional cryptocurrency system with privacy protection. Unlike other approaches, their system encodes event outcomes as part of a cryptocurrency note in a UTXO-based system [16].

Perry (2022) explores the concept of cryptocurrency wallets, describing them as souped-up flash drives that securely hold private keys for accessing cryptocurrency data stored in the blockchain [17].

Table 1. Approach Based Comparison

Author Name	Year	Main Concept	Objective	Findings
Takahashi and Lakhani	2019	Increasing use of cryptocurrencies and security challenges in online	Propose a method for conducting multiple-layered security	Focus on the challenges of maintaining security in online transac-

		transactions.	analyses, particularly for cryptocurrency exchange services.	tions and propose a method for enhanced security analyses in cryptocurrency exchange services [13].
Sai et al.	2019	Examination of security profiles in commonly used Android cryptocurrency applications.	Compare findings to control tests across cryptocurrency wallets, evaluating both security and privacy features.	Despite limited functionality, traditional financial services apps are marginally better in security but offer greater privacy measures [14].
Azman and Sharma	2020	Discussion on Bitcoin's transformative potential in the global economy and the introduction of HCH DEX for secure cryptocurrency storage.	Present a unique way to securely store cryptocurrency with a smart card setup for two-way authentication, aiming for an economically fair environment.	Introduction of HCH DEX as a secure method for storing cryptocurrency, resisting fraudulent and unethical policies [15].
Karanjai et al.	2021	Design and implementation of a conditional cryptocurrency system with privacy protection.	Introduce a system encoding event outcomes in a cryptocurrency note in a UTXO-based system.	Proposal and implementation of a conditional cryptocurrency system with privacy protection, different from approaches depending on smart contracts [16].
Perry	2022	Exploration of the concept of cryptocurrency wallets and their function as secure data holders.	Describe cryptocurrency wallets as souped-up flash drives holding private keys for accessing blockchain-stored data.	Explanation of cryptocurrency wallets as secure data holders, functioning like souped-up flash drives [17].

Table 1 reveals various approaches to enhancing cryptocurrency security and functionality, highlighting distinct contributions from different studies. Takahashi and Lakhani (2019) emphasize the need for multi-layered security analyses in cryptocurrency exchanges to address online transaction challenges, while Sai et al. (2019) identify a trade-off between security and privacy in Android cryptocurrency applications, suggesting the need for improved balance. Azman and Sharma (2020) introduce HCH DEX, a hardware-based solution for secure cryptocurrency storage, addressing fraud and unethical practices, whereas Karanjai et al. (2021) present a conditional cryptocurrency system with privacy protection, offering an alternative to traditional smart contract methods. Perry (2022) explains cryptocurrency wallets as secure data holders akin to advanced flash drives, underscoring their role in safeguarding private keys. Collectively, these studies highlight ongoing advancements and gaps in cryptocurrency security, including the need for practical multi-layered security frameworks, optimal security-privacy balance, scalable hardware solutions, integration of privacy-enhancing technologies, and advanced wallet security measures.

3 Proposed Work

User Identification Process and Picture-Based String Authentication Algorithm

A. User Identification Process using BLAKE2b-512 Hash

Input

- User identity information: **U** = (username, email, or unique identifier)
- User password in plaintext: **P**

Process Steps

Generate BLAKE2b-512 Hash for User Identity

- Apply the BLAKE2b-512 hash function to **U**:

$$\mathbf{H}_{\text{ID}} = \text{BLAKE2b-512}(\mathbf{U})$$

- Convert **U** into a fixed-length hash value using the BLAKE2b-512 algorithm:

$$\mathbf{H}_{\text{ID}} \in \mathbb{Z}^{512}$$

- The resulting hash $\mathbf{H}_{\text{ID}}$ serves as a unique and secure representation of the user's identity.

Generate MD5 Hash for User Password

- Simultaneously, generate an MD5 hash for **P**:

$$\mathbf{H}_{\text{PW}} = \text{MD5}(\mathbf{P})$$

- MD5 produces a 128-bit hash value:

$$\mathbf{H}_{\text{PW}} \in \mathbb{Z}^{128}$$

Store Hashes in the User Database

- Store $\mathbf{H}_{\text{ID}}$ and $\mathbf{H}_{\text{PW}}$ in a secure user database:

$$\mathcal{D} = \{(\mathbf{H}_{\text{ID}}, \mathbf{H}_{\text{PW}})\}$$

- This database $\mathcal{D}$ serves as a repository for user information, ensuring that sensitive details are not stored in plaintext.

Output

- $\mathbf{H}_{\text{ID}}$ and $\mathbf{H}_{\text{PW}}$ are stored in $\mathcal{D}$ for future reference during authentication and transaction verification processes.

B. Picture-Based String Authentication Algorithm

User Selection of Pictures

- During authentication, the user is presented with the same set of pictures $\mathcal{P}$ they selected during registration.

User Clicks on Predefined Areas

- The user clicks on predefined areas within $\mathcal{P}$, corresponding to the coordinates $\mathbf{C}$ where text was assigned during registration.

Pattern Formation During Authentication

- As the user clicks on the predefined areas $\mathbf{C}$, the authentication pattern $\mathcal{A}$ is dynamically formed:

$$\mathcal{A} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_n\}$$

- The system records the sequence of clicked areas:

$$\mathcal{A} \subset \mathbb{R}^2$$

Comparison with Registered Pattern

- The formed pattern $\mathcal{A}$ during authentication is compared with the registered pattern $\mathcal{A}_{\text{reg}}$:

$$\mathcal{A} \stackrel{?}{=} \mathcal{A}_{\text{reg}}$$

- If $\mathcal{A} = \mathcal{A}_{\text{reg}}$, authentication is successful.

Access Granted/Denied

- Based on the comparison result, access is granted if $\mathcal{A} = \mathcal{A}_{\text{reg}}$ and denied otherwise:

$$\text{Access} = \begin{cases} \text{Granted} & \text{if} \mathcal{A} = \mathcal{A}_{\text{reg}} \\ \text{Denied} & \text{otherwise} \end{cases}$$

Definitions

- **BLAKE2b-512 Hash:** A cryptographic hash function $H: \mathbb{D} \to \mathbb{Z}^{512}$ that transforms input data into a fixed-length hash value, providing a unique representation of the input's identity.
- **MD5 Hash:** A widely used hash function $H: \mathbb{D} \to \mathbb{Z}^{128}$ that produces a 128-bit hash value, commonly used for adding a layer of security to passwords.
- **Picture-Based String Authentication:** An authentication method where users select and interact with predefined areas on pictures to form a dynamic pattern for identity verification.

The proposed algorithm effectively enhances user authentication through a combination of robust cryptographic techniques and intuitive visual interaction. By employing the BLAKE2b-512 hash function for user identity, the algorithm ensures a highly secure and unique representation of user data, addressing concerns about data integrity and privacy with its 512-bit hash output. Simultaneously, the use of MD5 hashing for user passwords adds an additional layer of security, though MD5's susceptibility to vulnerabilities suggests the potential benefit of considering more secure alternatives like SHA-256. The picture-based string authen-

tication method leverages a user-friendly approach where authentication is based on interacting with predefined areas within selected images, thus creating a dynamic and personalized verification pattern. This visual interaction not only enhances security by requiring users to replicate a specific click sequence but also improves usability by engaging users in a familiar and straightforward process. However, while the visual pattern approach adds a layer of convenience and reduces reliance on traditional passwords, its effectiveness depends on the accuracy of pattern recognition and the security of the image selection and interaction process. Overall, the algorithm's combination of cryptographic hashing and visual authentication provides a comprehensive and user-centric approach to secure identity verification, though ongoing evaluations and updates are necessary to address potential weaknesses and adapt to evolving security threats.

Implementation Work

In Figure 1, the user registration process is illustrated with a focus on capturing and securing various user information, including username, password, email ID, and a biometric fingerprint image. The registration form includes fields for these details, with special attention to password and biometric handling. The entered password undergoes MD5 hashing, a widely used cryptographic hash function, providing a fixed-size 128-bit hash value. The biometric fingerprint image is hashed using Blake2B, another cryptographic hash function that produces a variable-size hash, ensuring a secure representation of the fingerprint data. A slider-based character extraction mechanism allows users to determine the level of granularity for character extraction from the Blake2B hash, enhancing security.

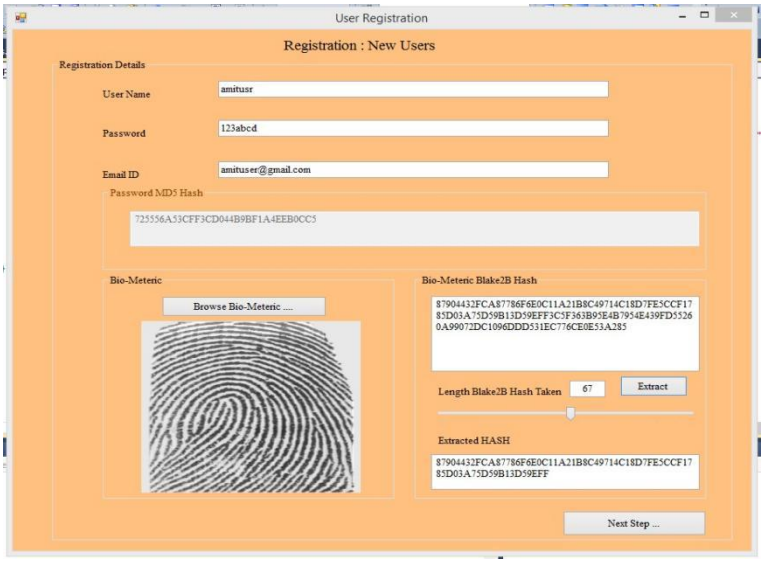

Fig 1. Registration Process 1

The hashed passwords and fingerprint data are securely stored in the database, employing practices like salting for password hashing. During transmission, sensitive data is encrypted using secure protocols like HTTPS. User-friendly error messages are implemented for validation issues to guide users through the registration process effectively.

The second step of the registration process introduces a visual verification mechanism, enhancing security through personalized pattern creation. Users start by selecting an image from a set of options, which serves as the basis for their unique pattern. The chosen image is then segmented based on the user's interaction, with each segment representing a distinct part of the image. For each segment, users associate specific text or alphanumeric characters, creating a mapping between visual elements and characters. As users select segments and associate text, a dynamic pattern is formed by combining the associated text for each selected segment. Users review and confirm the generated pattern to ensure accuracy. The completion of this step allows users to finalize their registration by providing additional required information. The system stores the created pattern, serving as a visual authentication method for subsequent logins or interactions. Overall, this visual registration process adds a layer of security by incorporating a unique, user-specific visual element into the authentication mechanism.

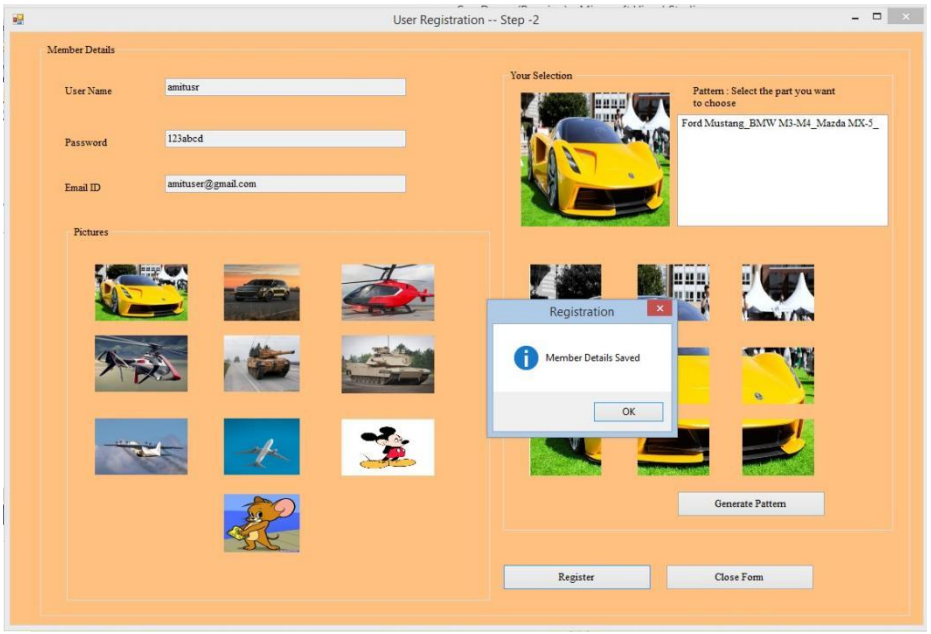

Fig 2. Registration Process-2

4 Result Analysis

Fingerprint File and Hash Generation:

- The proposed workflow begins with the submission of a fingerprint file by the user.
- The system generates a hash from the provided fingerprint file. This hash serves as a unique identifier for the user's fingerprint data.
- 906deda566ba5cb8f93744b600633db7fedf30576c9cd3570aa73fcfd0bc37ce0b904ae192c42108f62efa083b56f2b0d904b90b1b399af57627d689bb5788cb

Now we have extracted 54 characters from the hash 906deda566ba5cb8f93744b600633db7fedf30576c9cd3570aa73

Extraction of Characters from the Hash:

- From the generated hash, the system extracts the first 54 characters.
- These characters likely contain sufficient entropy to serve as a unique identifier while minimizing the length of the authentication string.

Image Division and Selection:

- The system utilizes an image, presumably of a Ford car, for additional authentication.
- The image is divided into nine distinct parts or sections.
- The system selects specific parts of the image based on predefined criteria. In this case, parts 3, 5, 7, and 8 are chosen for further processing.

Association of Text with Selected Parts:

- For each selected part of the image, the system associates specific text related to the content or characteristics of that part.
- Part 3 is associated with the text "backmachine."
- Part 5 is associated with the text "automobiles."
- Part 7 is associated with the text "chasispart."
- Part 8 is associated with the text "bumperback."
- These associations likely serve to create a contextual link between the image and the authentication process.

Formation of a Pattern:

- Based on the associated text from each selected part of the image, the system constructs a pattern.
- The pattern likely combines the textual associations with identifiers related to the image, such as the make and model of the car.

In our example, the pattern formed is
"Ford_Mustang_3_backmachine_5_automobiles_7_chasispart_8_bumperback."

Creation of the Final Blockchain for User Authentication:

- Integrating the username, extracted hash, and formed pattern, the system constructs the final blockchain entry for user authentication.
- The blockchain entry serves as a secure and tamper-evident record of the authentication process.

In our example, the final blockchain entry for the user with the username "aks123" is:

aks123_906deda566ba5cb8f93744b600633db7fedf30576c9cd3570aa73_Ford_Mustang_3_backmachine_5_automobiles_7_chasispart_8_bumperback

Entropy in the context of information theory refers to the measure of uncertainty or randomness in a sequence of symbols or data. It's often used to gauge the strength of passwords or cryptographic keys, indicating how difficult it would be to guess or crack them.

In the provided pattern:

"aks123_906deda566ba5cb8f93744b600633db7fedf30576c9cd3570aa73_Ford_Mustang_3_backmachine_5_automobiles_7_chasispart_8_bumperback"

Each character, whether it's a letter (uppercase or lowercase), a digit, or an underscore, contributes to the overall entropy of the pattern. Entropy is calculated based on the number of possible symbols and the probability distribution of those symbols.

Results of Analysis from some of the testing tools :

- 1,216,796,999 septuagintillion years (from comparitech.com):
- This estimation suggests that it would take an unfathomably long time to crack the pattern, indicating a very high level of security.
- It's important to note that this estimation is based on assumptions about the computational power of potential attackers and their ability to try different combinations.
- 2 trillion trillion trillion trillion trillion trillion trillion trillion trillion years (from passwordmonster.com):
- Similarly, this estimation underscores the extreme difficulty of cracking the pattern, emphasizing its robustness against brute-force attacks.
- 832.43 bits of entropy (from insecure.in):
- This entropy measurement quantifies the unpredictability or randomness of the pattern.
- A higher entropy value indicates a stronger password or pattern.
- 796 bits of entropy (from rumkin.com):
- Again, this value confirms the high level of unpredictability in the pattern, making it highly resistant to attacks that rely on guessing or brute-force methods.

Table 2. Entropy Bits Comparison

	insecure.in	rumkin.com
Entropy Bits	832.43	796

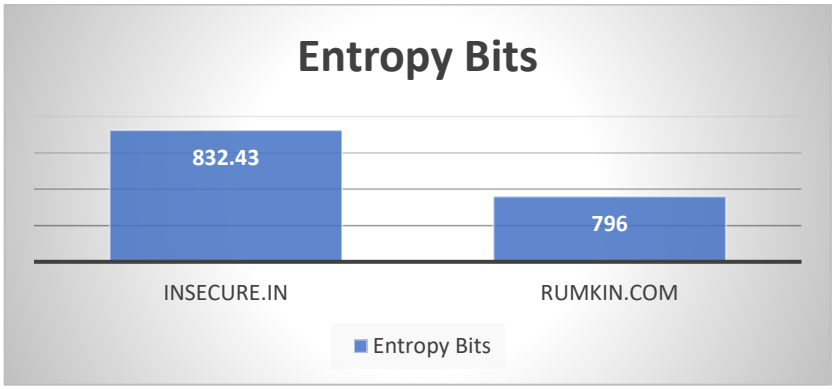

Figure 1. Comparison Graph in Entropy Bits

The result analysis demonstrates the effectiveness of the proposed algorithm in enhancing user authentication through a multi-faceted approach. By generating a unique hash from user fingerprint data and extracting a 54-character substring, the system creates a distinct identifier for each user. This identifier is then integrated with a picture-based authentication process, where selected image parts and associated text form a complex pattern, such as "Ford_Mustang_3_backmachine_5_automobiles_7_chasispart_8_bumperback." The final authentication string combines the username, hash, and formed pattern, creating a tamper-evident blockchain entry. The analysis shows that the entropy of the resulting pattern is exceptionally high, with estimates of 832.43 bits and 796 bits, confirming the robustness of the authentication mechanism. Computational estimates suggest that cracking the pattern would require an impractically long time, ranging from 1.2 sextillion years to 2 trillion trillion trillion trillion trillion trillion trillion trillion trillion years. These results

highlight the algorithm's strong security features, including its resilience to brute-force attacks and high unpredictability, ensuring a secure and reliable authentication process.

5 Conclusion

The proposed algorithm represents a significant advancement in user authentication technology by integrating BLAKE2b-512 hashing, MD5 hashing, and a picture-based string authentication method. The use of BLAKE2b-512 for generating a unique hash from user identity information ensures a high level of security through its robust cryptographic properties, while MD5 hashing provides an additional layer of protection for user passwords. The incorporation of a picture-based authentication system further enhances the security mechanism by creating a dynamic and contextually enriched authentication pattern. This approach leverages both text and image data, resulting in a complex pattern that is difficult to replicate or compromise. The result analysis confirms the effectiveness of the proposed system, demonstrating an extraordinarily high level of security with entropy values indicating strong resistance to brute-force attacks. The final blockchain entry for authentication not only secures user data but also provides a tamper-evident record, reinforcing the integrity and reliability of the authentication process. Overall, the algorithm's design successfully addresses the need for a more secure and sophisticated user authentication method in the digital landscape.

Future work in this domain could explore several avenues to further enhance the proposed algorithm and address potential areas for improvement. One promising direction is the integration of biometric data beyond fingerprints, such as facial recognition or iris scans, to create a multi-modal authentication system. This could provide an additional layer of security and convenience for users. Another area of interest is the optimization of the picture-based authentication method to support a broader range of image types and enhance user experience. Research could also focus on refining the hashing algorithms, including evaluating the potential benefits of newer cryptographic functions or combining multiple hash functions to achieve even higher security levels. Additionally, implementing and testing the proposed algorithm in real-world scenarios would provide valuable insights into its performance, usability, and scalability. This could include pilot studies across different industries and user demographics to assess the algorithm's effectiveness in various contexts. Finally, exploring the integration of the algorithm with emerging technologies, such as blockchain-based decentralized identity systems or artificial intelligence-driven security measures, could further enhance its robustness and adaptability in the evolving digital landscape.

6 Author Contributions:

Aakansha Mitawa: Conceptualization, Problem formulation, Methodology, Original draft preparation, Reviewing and Editing, and Final drafting, Data curation, Programming, Simulation, Validation, Numerical analysis, Visualization, and System setup.
Dr. Pawan Bhamu: Supervision,Validation,Writing, Reviewing.

7 Acknowledgment:

In conducting this research on “Designing Secure Financial Transaction Using Blockchain” , no external funding was received from any organization. The research was self-funded by the authors.

8 conflict of Interest:

There is no conflict of interest among the authors.

9 Ethical Approval:

This approach ensures transparency, accountability, and ethical responsibility in advancing knowledge and practice in this field.

10 Data Availability:

The data supporting this study's findings are available from the corresponding author upon reasonable request.

11 Replication of Results:

This is code which designed in Visual Studio and its database is developed in SQL Server. We have make use to the libraries provided by language C# for the hashing functions and graphical user interface and image manipulation. Sibnce , its is not the open source code shared on open platform so we cannot provide the source code. But references of the packages and name spaces used, we listing below,

- System.IO: For working with files, directories, and streams.
- System.Text: For string manipulation (like concatenation, searching, formatting).
- System.Collections.Generic: For generic data structures like List<T>, Dictionary<TKey, TValue>.
- System.Linq: Offers extension methods for working with collections (like Where, Select, Join).
- System.Net: For network communication (sockets, HTTP requests).
- System.Threading: For multithreading functionalities.

• System.Security.Cryptography Namespace: This namespace provides classes for various cryptographic functionalities, including several hash functions

References

1. Hertzog, E., Benartzi, G., & Benartzi, G. (2018). Bancor protocol: Continuous liquidity for cryptographic tokens through their smart contracts (Tech. Rep.).
2. Adams, H., Zinsmeister, N., & Robinson, D. (2020). Uniswap v2 core (Tech. Rep.).
3. Egorov, M. (2019). Stableswap-efficient mechanism for stable-coin liquidity (Tech. Rep.).
4. Krishnamachari, B., Feng, Q., & Grippo, E. (2021). Dynamic curves for decentralized autonomous crypto-currency exchanges.
5. Spithoven, A. (2019). Theory and reality of cryptocurrency governance. Journal of Economic Issues, 53(2), 385-393.
6. Greenberg, A. (2011). CryptoCurrency. Forbes. Archived from the original on 31 August 2014.
7. Farell, R. (2015). [Crypto currency] (Unpublished manuscript). University of Pennsylvania Scholarly Commons.
8. Liu, Y., & Tsyvinski, A. (2018). Risk and Returns of Cryptocurrency.
9. Halpern, S. (2018). Bitcoin Mania. The New York Review of Books, 65(1), 52-54, 56.
10. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press.
11. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
12. Sauer, B. (2016). Virtual currencies, the money market, and monetary policy. International Advances in Economic Research, 22(2), 117-130.
13. Takahashi, H., & Lakhani, U. (2019). Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers. In 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE) (pp. 71-73). Osaka, Japan: IEEE.
14. Sai, A. R., Buckley, J., & Le Gear, A. (2019). Privacy and Security Analysis of Cryptocurrency Mobile Applications. In 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ) (pp. 1-6). Miami Beach, FL, USA: IEEE.
15. Azman, M., & Sharma, K. (2020). HCH DEX: A Secure Cryptocurrency e-Wallet & Exchange System with Two-way Authentication. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 305-310). Tirunelveli, India: IEEE.
16. Karanjai, R., Xu, L., Gao, Z., Chen, L., Kaleem, M., & Shi, W. (2021). On Conditional Cryptocurrency With Privacy. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-3). Sydney, Australia: IEEE.
17. Perry, T. S. (2022). A Bitcoin Wallet for the Masses: Square simplified credit-card transactions. Now it wants to build cryptocurrency hardware. IEEE Spectrum, 59(1), 42-43.