Adopting Blockchain for Enhancing Data Security and Privacy in Service-Based Digital Platforms: A Case Study of a Distributed Application (Dapp) Global Mission Services

Yves Bizumuremyi(✉), Ntima Mabanza, and Muthoni Masinde

Department of Information Technology, Central University of Technology, Free State Private Bag X20539, Bloemfontein 9300, South Africa
yvesbizu@gmail.com, {nmabanza,emasinde}@cut.ac.za

Abstract. This research aims to assess the viability of Blockchain technology for improving data security within service-based digital platforms. The methodology includes a literature review to identify blockchain trends and data security problems, surveys to assess possible platform use and user perceptions of online security, and the development of a digital platform prototype for Global Mission Services (GMS). Survey responses are compared statistically to determine user attitudes. The findings show that using the Blockchain-based distributed application (Dapp) platform improves data security significantly. There is significant interest in its implementation, particularly in light of growing concerns about online security. The GMS prototype demonstrates successful missionary service integration while overcoming accessibility barriers. These findings align with previous studies on Blockchain's security benefits, underlining its importance in service-based digital platforms and shared economies. The study emphasises Blockchain's potential in data security and proposes the Ethereum-based Dapp platform as a promising approach to improve security and stimulate greater adoption of service-based digital platforms.

Keywords: Blockchain Technology · Data Security · Shared Economy · Missionary Services · Distributed application (Dapp) · Digital Platform · Eswatini · South Africa

1 Introduction

A wide range of services are now easily accessible to a larger audience through digital channels because of the expansion of service-based digital platforms in recent years, which has changed how business is conducted [1, 2]. However, this quick transition to the digital age has also increased cyberattacks and unwanted access attempts. These digital platforms manage enormous volumes of private information, raising worries about data security and privacy violations. This problem is especially important in the context of

M. Masinde et al. (Eds.): AFRICATEK 2023, LNICST 520, pp. 57–70, 2024.
https://doi.org/10.1007/978-3-031-63999-9_4

missionary work in Eswatini and South Africa, where essential services are not accessible due to a lack of access to information about these services. Eswatini and South Africa were chosen as case study regions due to their practical accessibility, facilitating precise data collection and direct engagement with missionaries. This approach aims to better understand and address the challenges they encounter in accessing essential services. The paper suggests a novel approach to solve this problem: a decentralised application (Dapp) platform built on the Ethereum Blockchain. Increased confidentiality, immutability, and transparency are all features of this Dapp platform, which combines numerous missionary activities under one digital platform. This platform seeks to improve accessibility and effective resource use while reducing data security and privacy issues by utilising the benefits of blockchain technology.

Blockchain technology has drawn much attention from scientists in several research fields, and it is expected to be crucial in determining the direction of the upcoming wave of digital platforms [3]. Ethereum stands out among the different blockchain frameworks available for its potential to produce Dapps that are reliable, secure, and open [4]. Dapps are naturally resistant to traditional security problems like hacking and data breaches associated with centralised platforms because they are backed by smart contracts and distributed networks [5]. The data security and privacy issues that affect service-based digital platforms, especially those that cater to missionary activities, can be successfully solved by implementing a Dapp platform built on the Ethereum blockchain. This paper describes the creation of such a Dapp platform and emphasises how blockchain technology may be used to improve accessibility, transparency, data security, and privacy protection.

1.1 Objectives

The main objective of this study is to investigate the viability of using blockchain technology to enhance data security and accelerate the uptake and utilisation of service-based digital platforms in Eswatini and South Africa. The study aims to achieve the following specific objectives:

1. Conduct a literature review to identify current trends, concerns, ongoing blockchain technology and data security research, and missionary activities in South Africa and Eswatini.
2. Evaluate the effectiveness of the Dapp platform based on the Ethereum Blockchain in providing trust and data integrity for service-based digital platforms.
3. Develop a prototype of the GMS digital platform that integrates missionary services under a single platform to enhance access and efficient utilisation of the massive resources under the care of missionaries.

2 Literature Review

2.1 Missionaries' Activities

According to Jasmine Senior (2021), Missionaries love and follow Jesus wherever they are while demonstrating love for others throughout their lives. They help communities get better and grow by engaging in missionary work. All around the world, there are

missionaries. According to David Maxwell (2014), missionary movements and activities significantly impacted the lives of numerous people worldwide, influencing the course of world history.

Among the many services provided by missionaries in Eswatini and South Africa are those related to health, education, the environment, accommodation and feeding people without homes, drug rehabilitation, helping refugees, early childhood development programs, managing orphanages, stopping human trafficking, communication, and neighbourhood improvement projects. This study focuses on the logistical services travelling missionaries provide to members of their networks as they trade services within their religious group. Many service-based internet platforms today provide specialised services, such as Airbnb and booking.com. Missionaries advertise their services and activities through personal websites or social media. The limitation of this is that the information is not easily found online. The study's findings will be demonstrated on a logistic travel system incorporating all the missionaries' services into one platform.

2.2 Blockchain Technology

Blockchain is a decentralised system built on the concepts of peer-to-peer networks and cryptographic fundamentals like asymmetric encryption and digital signatures. It allows users to communicate and record transactions without restriction or collaboration. In a blockchain architecture, it is possible to choose which valid information is added to the distributor and disseminated across the participant's network using a secure, associated database based on a consensus process [6].

2.2.1 Current Trends in Blockchain Technology and Its Applications in Data Security

The realm of data security has undergone a seismic shift. Thanks to the advent of blockchain technology, which has skyrocketed in popularity over the past several years. Numerous studies have confirmed this game-changing innovation's potent and fast-rising nature within the data protection sphere. This section will delve into many blockchain trends currently observed vis-à-vis applications for securing valuable information.

One of the prevailing trends in blockchain technology is the surge in its utilisation for Dapps. Essentially, Dapps are systemic solutions operating within blockchain networks with immutability, security, and transparency as key facets [7]. Considering Blockchain's dependability and versatility attributes, Dapps can be created effortlessly to safeguard sensitive information while reinforcing safe transactions among users from any location [8].

Another prevailing development in Blockchain Technology pertains to smart contract adoption. These computer programs, also known as self-executing contracts, present possibilities for process automation, such as enforcement and authentication of agreements [9]. Intermediaries or authorities are not required. Smart contracts accomplish data protection and assure transaction execution according to pre-established policies. Deployment of smart contracts can scale down administrative overheads and refine operational efficiencies while mitigating potential technical shortcomings or risks in transactional undertakings [10].

One more trend is that blockchain technology can potentially improve data sharing trust and transparency [11]. Blockchain could be used to build a decentralised network that enables secure data sharing between parties without intermediaries [12]. This is especially useful in low trusts, such as cross-border transactions.

2.2.2 Ongoing Research and Development in Blockchain-Based Solutions for Data Security

Recently, blockchain technology has attracted much attention from researchers due to its potential for data security. Extensive research and development efforts have been invested in exploring blockchain-based solutions for securing sensitive information. One specific area of focus includes creating consensus algorithms that can enhance the scalability and efficiency of blockchain networks [13]. By executing this, more transactions could be efficiently handled concurrently, thus enhancing overall performance.

Another crucial advancement involves developing privacy-preserving technologies for maintaining secure yet anonymous data sharing [14], which adheres to preserving sensitive details. In utilising this innovation, the integrity of all pieces interchanged is secure, while decentralised approaches now ease information management via blockchain technology. Researchers are currently investigating how they can use these advancements in various spheres, such as supply chain management or healthcare, among other aspects [15], to increase data security levels and establish transparency. It all defines an increased efficiency rate plus Secured means towards managing important confidential materials promoting utmost assurance.

2.3 Ethereum

Ethereum [16] is a representative public blockchain using a PoW (Proof of Work) consensus algorithm like Bitcoin. The PoW consensus algorithm is the method blockchain networks use to choose blockmakers from among untrustworthy members. To choose a miner, participants compete to find a hash value that fulfils the desired requirement. The public Blockchain presents the idea of cryptocurrency's economy, which promotes the right consensus by paying the chosen miner in bitcoin. The previous block's integrity is ensured by connecting the newly created block to the previous block using the "previous block hash" found in the block header before being disseminated to the blockchain network's users. The decentralised network continually advances without administrators; all blocks and transactions are publicly available.

Ethereum supports creating and distributing smart contracts [17] for developing DApps. A smart contract is written in Solidity, a Turing completeness language, and recorded in the distributed ledger to ensure the integrity of the results according to automated execution and input [18]. Figure 1 represents the operation of the smart contract in Ethereum. The smart contract made with Solidity is compiled and stored as the EVM (Ethereum Virtual Machine)-bytecode in the ledger. Calling the code through Ethereum clients such as Geth (Go-Ethereum) is executed in the EVM environment.

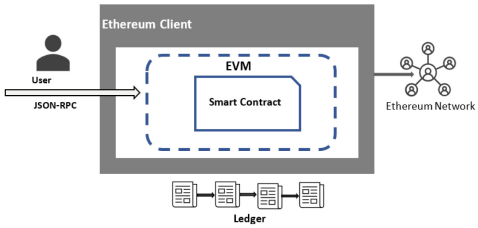

Fig. 1. Ethereum framework architecture

2.3.1 Ethereum Blockchain Mechanism to Ensure the Security of Information

- Cryptography and encryption: These provide security services like confidentiality, non-repudiation, authentication, and authorisation [19].
- Consensus mechanisms: These algorithms determine whether to accept a new block of verified transactions onto the chain [20].
- Timestamp and hashing of the previous block: This safeguards data integrity. Due to consistent and immutable data provenance, the blockchain structure aids in tracking back to a specific transaction [21].

The three initial building blocks of a blockchain are depicted in Fig. 2.

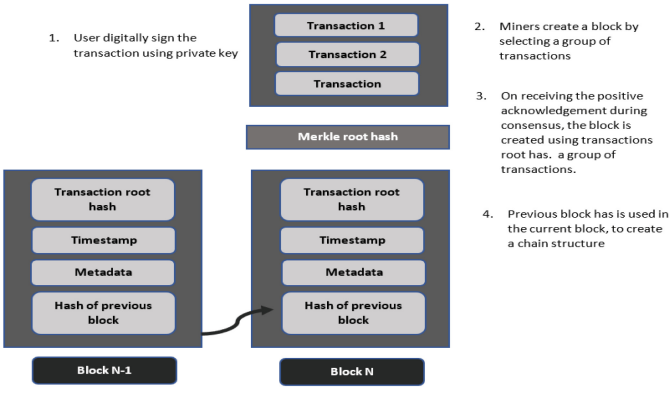

Fig. 2. Building blocks of a blockchain.

Blockchain technology employs a linked list data structure. Transactions are validated by the Blockchain's participant nodes [22]. Each block is hashed to preserve confidentiality and contains a group of legitimate transactions. The chain of blocks that forms, resembling a linked list structure, each holds the hash computed by the preceding block. Every valid transaction is kept track of in every block. The hash value is significantly affected by any hacker effort to alter the data. Each block is guaranteed to be valid by requiring consent from every other node in the chain when a new block is added to

the chain [23]. Figure 3 demonstrates this. Any blockchain member can play one of two key roles, which are described below:

Initiate transaction: The Blockchain cannot be active or activated unless the participant starts a transaction. Other blockchain network users then confirm the transaction.

Participants can take on the role of miners by broadcasting and confirming transactions, competing to add a block, and broadcasting new blocks.

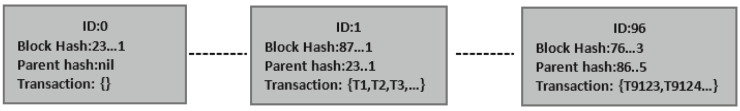

Fig. 3. Blockchain example

The use of blockchain technology in digital platforms such as the GMS platform offers tremendous prospects to improve the existing status of missionary travel. Sensitive data can be securely saved, viewed, and shared only with authorised individuals by exploiting Blockchain's decentralised and transparent characteristics, improving data security and privacy within the missionary ecosystem. Furthermore, Blockchain's immutability and smart contract capabilities enable transparent tracking and verification of resources, encouraging accountability and expediting processes. This disruptive technology can potentially change missionary services in South Africa and Eswatini by increasing data security, resource allocation, and general efficiency.

3 Methodology

This study integrated a thorough literature review, survey, and design works as part of a mixed-methods strategy. This study aimed to determine whether blockchain technology can improve data security and integrity in service-based digital platforms and examine how the GMS platform might be used to deliver vital services to missionaries in South Africa and Eswatini.

3.1 A Literature Review

As mentioned earlier, a mixed methodology was used for this study, including a literature review. A thorough literature study was done to determine the trends, issues, and active research in the areas of blockchain technology and data security in digital platforms. For the aim of this review, electronic databases like IEEE Xplore, ScienceDirect, and Google Scholar were used. Papers that were deemed pertinent to the study's aims and published between 2016 and 2022 made up the review criteria. The main key words were "Blockchain" and "Data Security".

3.2 Survey

Apart from the systematic literature review, surveys were used as part of this study to achieve the research objective. The survey was sent online using Google Forms and distributed to potential GMS platform users through social media such as WhatsApp and email. The collection of data was done in two phases. The first phase aimed at identifying different GMS potential digital platform users around South Africa and Eswatini. This assisted the researcher in learning more about existing missionary centres in South Africa and Eswatini, including the different types of activities conducted by those missionary centres. The second phase aimed at identifying the users online experience with their current website. To get a better understating, in the first phase the survey incorporated questions that sought to collect more detailed information about these missionary centres, such as their details, geographical location, operational data, how long they have been existing, staff number, monthly income, type of services provided, and level of technology adoption (i.e., they had a website or not). In the second phase the survey incorporated question about the perceptions and practices in relation to confidentiality, integrity, and availability within the users' online platforms. The first phase involved 80 missionary centers, with 62 participants completing the survey, and the second phase targeted 50 missionary centers selected based on their website presence and demonstrated knowledge of online security.

Data collected from the survey were examined using R studio 4.0.5. (Team, 2015). Quantitative data from the majority of the questions were imported into Excel for preliminary analysis. Kolmogorov-Smirnov and Shapiro's tests were used to ascertain how the data were distributed. The results were presented using charts and graphs, and the findings were discussed in relation to the study objectives.

3.3 Design Work

This study used a design approach that included the development of a Dapp on the Ethereum blockchain in addition to the literature review and survey method. This Dapp used Ethereum's security and transparency to enable secure and decentralised transactions while resolving issues raised in the survey. The Dapp design, guided by past literature, aims to deliver a well-informed solution associated with research objectives, while also contributing a multi-faceted methodology to issue resolution.

4 Survey Results and Findings

4.1 Selection Results

Geographical Distribution: Most of the missionary centres in the study were in South Africa (95.31%), whereas Eswatini (4.69%) represented a minor part. Most centres (84%) were in Africa, with some also operating in the SADC region and others operating globally (14.1%).

Operational Details: According to the investigation, many of the facilities had been in operation for more than 20 years, demonstrating their longstanding presence. Most

centres (40.6%) had between 11 and 20 employees, and 45.3% had monthly income between R 50,000 and R 100,000. The right-skewed distribution of the data indicated the lifetime of most centres. All centres provided workshop and retreat facilities, primarily for religious purposes.

Website Information: Most centres (76.6%) had up and running websites; the others did not. The monthly revenues of centres with websites tended to be more significant, with many of them reaching R 50,000. Increased accessibility and money were strongly connected with website presence. Monthly revenue for a centre was likewise connected with the number of employees.

4.2 Online Security and Website Usage

52% of respondents said they utilised their websites primarily for advertising. Most users (56%), compared to 16% each for tablets and mobile devices, controlled their websites using PCs. The information showed that the experiences of respondents with online security could be summed up as follows:

1. Confidentiality (Mean: 2.996, SD: 0.8525530)
2. Integrity (Mean: 3.144, SD: 0.8038837)
3. Availability (Mean: 2.935, SD: 0.9816742)

In the evaluation of confidentiality, respondents expressed worries about the security of their passwords (mean: 2.74) and the privacy of the internet (mean: 3.92), as well as caution regarding data protection rules (mean: 2.8) and their comprehension of how website owners use their own data (mean: 2.94). Respondents prioritised online business security (mean: 3.32) and paid attention to security during online transactions (mean: 3.14), respectively, regarding integrity. There was space for improvement in the configuration of the available security settings (mean: 2.68), and instances of data compromise were reported (mean: 3.2), even though they demonstrated expertise in configuring digital platform security measures (mean: 3.38). Participants discussed previous incidents of website hacking (mean: 2.92) and prohibited website access (mean: 2.82), with some respondents citing unintentional redirection to alternative websites (mean: 2.8) in terms of availability. These results show the variety of viewpoints and experiences that exist in the field of website usage and online security.

4.3 Selection Findings

Several essential considerations are considered when creating an integrated digital platform for missionary centres. The platform must first and foremost serve a geographically diverse user base predominantly centred in South Africa but also has a regional presence in other regions of Africa and the SADC. Robust data security procedures are therefore required to preserve user data and privacy. The platform must also be flexible enough to accommodate the missionary centres' diverse operational requirements and personnel sizes ranging from 11 to 50 persons. Robust data security and effective team coordination and communication are essential. Additionally, the platform's ability to boost sales through improved online visibility emphasises how crucial it is to design a captivating

user interface. These factors combine to create a holistic solution that satisfies the needs of both missionary institutions and visitors while utilising the security and accessibility advantages of blockchain technology, ultimately striving to be a game-changing solution.

4.4 Online Security and Website Usage Findings

According to the survey results regarding online security experience, proper password management is critical from a confidentiality aspect due to worries about online credential security. Passwords that are too simple to remember can jeopardise digital security. As a result, a user-centric platform with strong password tools and security awareness is critical. Users emphasise security in online transactions and configuration, yet data compromises highlight the need for improved protection systems. Incorporating user-friendly security measures can help to build a trustworthy digital ecosystem and increase engagement. Users' experiences with security lapses and outages emphasise the platform's need for robust cybersecurity that constantly enables the system to be online.

5 Prototype Development

The survey was vital in shaping the GMS Digital Platform's requirements. Missionaries from South Africa and Eswatini participated in a survey to understand their needs and services. The survey outcomes outlined key aspects of the platform:

1. **Easy access and Transactions:** The platform must offer user-friendly access and transaction capabilities tailored to missionaries' needs.
2. **Confidentiality:** Robust security measures are crucial to prevent unauthorised access and protect sensitive data.
3. **Data Integrity:** Ensuring reliable data and transactions is vital for user trust.
4. **Availability:** Maintaining seamless access is essential for missionaries' efficiency.

Considering the survey, the following development priorities are recommended:

1. **Data Integrity:** Address user concerns about data reliability.
2. **Confidentiality:** Prioritise password security, data protection, access prevention, and data loss prevention.
3. **Availability:** Enhance platform accessibility.

5.1 Blockchain Implementation in the Prototype to Ensure Data Security

The technology stack for the GMS Digital platform prototype comprises key components aligned with Blockchain. Addressing user requirements, we encompassed four framework components.

1. **Easy Access and Transactional Capabilities:** A user-friendly framework called ReactJS was selected for front-end development. Platform accessibility is improved with ReactJS, which enables smooth user interaction.

2. **Integrity:** Given the high mean score of survey's participants concerned about data integrity, Blockchain technology was critical in tackling the data security issue. Solidity was used to create smart contracts that assure secure transactions. Web3, a JavaScript library, facilitated blockchain integration, as highlighted in Sect. 2, allowing for transparent transactions.
3. **Confidentiality:** Based on the survey results, participants demonstrated the difficulty of using passwords which led to finding a tool that would help resolve the problem. MetaMask emerged as a robust tool, safeguarding user information.
4. **Availability:** Availability is also a crucial concern for the participants based on the results of the survey. To ensure decentralised, secure data storage, Infura IPFS (Inter-Planetary File System) was integrated. IPFS distributes data across nodes, enhancing data security and availability, and reducing the risk of loss or unauthorised access.

5.2 GMS Decentralised Architecture

The platform uses blockchain technology's inherent security capabilities to build a safe and tamper-proof data storage, management, and sharing environment. The Ethereum platform and Web3 client (Ethereum JavaScript API) were utilised in the study's implementation to connect with the front end of smart contracts running on Blockchain.

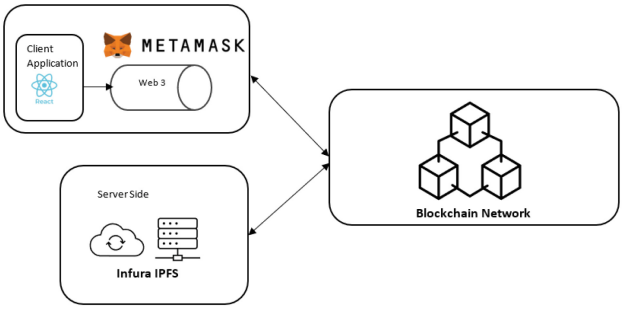

Fig. 4. GMS decentralised architecture

Figure 4 depicts the architecture diagram for the global mission digital platform. The client-side application, or front end, is built with ReactJS to ensure the platform has a user-friendly interface. It is hosted in the distributed network utilising Infura IPFS to ensure availability. The Ethereum blockchain network is used in the backend to ensure distributed server architecture. To ensure proper data protection, each node in the blockchain network retains a copy of the ledger and a smart contract. The platform is built on Ethereum and uses Metamask for authentication. Smart contracts are used for transactions.

5.2.1 System Design

Use Case Scenario: In this use case, Father John Doe and Sister Mary, who are both familiar with the GMS digital platform, serve as the host and guest, respectively. In order

to securely verify his identity on the Ethereum blockchain, Father John Doe decides to register his mission centre. He logs in using his Metamask wallet. Then lists accommodation options. Sister Mary logs in at the same time using the same secure method. In search of a suitable place to stay, she clicks on the "Accommodation" feature. She locates a nearby mission with the perfect lodging because she has faith in the platform's specialised services for Catholic missionaries. She smoothly makes a reservation and pays for her stay through the platform's integrated Metamask wallet, securely recording everything on the Blockchain.

Sister Mary uses the platform to interact with other missionaries while on the field, share her community volunteer activities, and market her services. The Blockchain's secure transactions ensure transparent interactions. Father John Doe and Sister Mary each have access to a decentralised, secure, and user-friendly networking and lodging option thanks to the GMS Digital Platform. The platform is well suited to meet the particular requirements of Catholic missionaries working in Swaziland and South Africa since it uses Blockchain, smart contracts, and Metamask integration.

Use Case Diagram
(See Fig. 5).

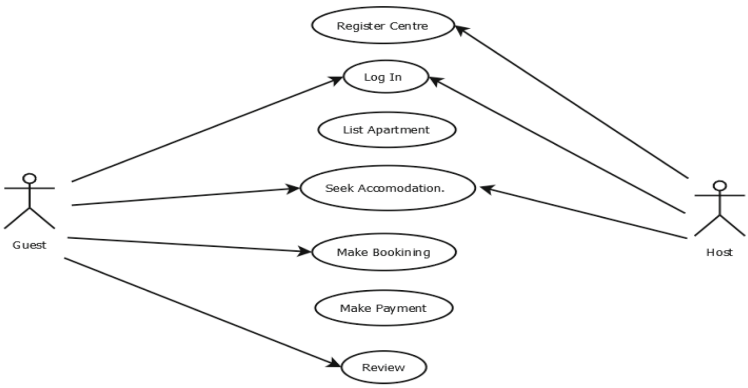

Fig. 5. GMS use case diagram

Class Diagram

The GMS platform's class diagram, shown in Fig. 6, includes the "Center," "Accommodation," "Host," and "Guest" smart contract classes. The figure shows relationship between "Accommodation" and both the "Host" and "Guest" classes as well as one-to-many relationships between "Center" and "Accommodation." While each "Accommodation" corresponds to a single "Center," each "Center" can link to several "Accommodations." Additionally, numerous "Hosts" and "Guests" can be connected to a single "Accommodation," allowing for complex interactions on the GMS platform.

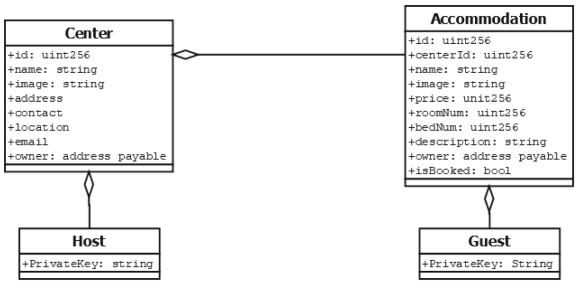

Fig. 6. Class Diagram

5.2.2 Prototype Implementation

The i5 Core processor, 8 gigabytes of RAM, and 250 GB Solid State Drive (SSD) of the laptop used to produce the prototype provided an appropriate balance of processing speed, memory, and storage space for the project's development requirements. ReactJs was used to construct the front end. The testing framework is Truffle, the backend was created in Solidy, and Infura IPFS is being used for distributed storage.

6 Conclusion

This study investigated the viability of a distributed application (Dapp) platform based on the Ethereum Blockchain as a solution to the data security and privacy concerns of service-based digital platforms. The study focused on the development of a prototype GMS digital platform that integrates missionary services under a single digital platform. The results and GMS platform prototype development demonstrated the effectiveness of the proposed Dapp platform in addressing data security and privacy concerns. The literature review revealed that blockchain technology is a disruptive technological advancement that can enhance data security and privacy in service-by digital platforms. The survey results imply that implementing the GMS digital platform incorporating all the missionaries' information can increase accessibility and greatly increase centres' income, enabling them to hire more staff, which will help reduce unemployment and offer greater services to their communities.

7 Limitations and Future Work

This study offered insightful information about the possible uses of blockchain technology for securing service-based digital platforms, but some limitations must be recognised. Firstly, the study's conclusions are based solely on a GMS digital platform prototype case study, which requires additional investigation to determine its potential efficacy and constraints in various scenarios. Secondly, the survey results of the study are based on a small sample number of users. Therefore, future research should also consider employing a bigger sample size to confirm the findings and further understand user perceptions, demands, and concerns related to adopting Dapp platforms. Lastly, the legal and regulatory issues associated with implementing blockchain technology in the shared

economy were overlooked. Future studies should investigate the conceivably necessary legal and regulatory frameworks for adopting Dapp platforms in the shared economy and any obstacles to adoption and successful implementation.

References

1. Burnod, P., Dugar-Zhabon, R.: Digital platforms in the B2b market. Mod. Technol. Sci. Technol. Progress **2022**(1), 333–334 (2022). https://doi.org/10.36629/2686-9896-2022-1-333-334
2. Tunggal, A.T.: What is the Cost of a Data Breach in 2022? | UpGuard (2023). https://www.upguard.com/blog/cost-of-data-breach. Accessed 3 April 2023
3. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat. Inform. **36**, 55–81 (2019). https://doi.org/10.1016/j.tele.2018.11.006
4. Huang, K., Ma, J., Wang, X.: A comparative analysis of bitcoin and ethereum blockchain. In: Proceedings - 2021 2nd international seminar on artificial intelligence, networking and information technology, AINIT 2021, pp. 678–682 (2021). https://doi.org/10.1109/AINIT54228.2021.00137
5. Chen, H., Pendleton, M., Njilla, L., Xu, S.: A survey on ethereum systems security: vulnerabilities, attacks and defences. arXiv: Cryptography and Security (2019)
6. Balaskas, A., Franqueira, V.N.L.: Analytical tools for blockchain: review, taxonomy and open challenges. In: 2018 international conference on cyber security and protection of digital services, cyber security 2018, pp. 1–8 (2018). https://doi.org/10.1109/CyberSecPODS.2018.8560672
7. Verma, S., Dash, S., Joshi, A., Kavita: A detailed study of blockchain and dapps. In: International Conference on Cyber Resilience, ICCR 2022, pp. 1–5 (2022). https://doi.org/10.1109/ICCR56254.2022.9996003
8. Udokwu, C., Anyanka, H., Norta, A.: Evaluation of approaches for designing and developing decentralised applications on blockchain. In: ACM International Conference Proceeding Series, pp. 55–62 (2020). https://doi.org/10.1145/3423390.3426724
9. Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., Wang, F.Y.: An overview of smart contract: architecture, applications, and future trends. In: IEEE Intelligent Vehicles Symposium, Proceedings, vol. 2018-June, pp. 108–113 (2018). https://doi.org/10.1109/IVS.2018.8500488
10. Zheng, Z., et al.: An overview on smart contracts: challenges, advances and platforms. Futur. Gener. Comput. Syst. **105**, 475–491 (2020). https://doi.org/10.1016/J.FUTURE.2019.12.019
11. Chowdhury, M.J.M., Colman, A., Kabir, M.A., Han, J., Sarda, P.: Blockchain as a notarization service for data sharing with personal data store. In: Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, pp. 1330–1335 (2018). https://doi.org/10.1109/TRUSTCOM/BIGDATASE.2018.00183
12. Huang, H., Chen, X., Wang, J.: Blockchain-based multiple groups data sharing with anonymity and traceability. Sci. China Inf. Sci. **63**(3), 1–13 (2020). https://doi.org/10.1007/S11432-018-9781-0/METRICS
13. Cachin, C., Vukolić, M.: Blockchain consensus protocols in the wild (Keynote Talk). DROPS-IDN/8016, vol. 91, pp. 1–16 (2017). https://doi.org/10.4230/LIPICS.DISC.2017.1
14. Bernabe, J.B., Canovas, J.L., Hernandez-Ramos, J.L., Moreno, R.T., Skarmeta, A.: Privacy-preserving solutions for blockchain: review and challenges. IEEE Access **7**, 164908–164940 (2019). https://doi.org/10.1109/ACCESS.2019.2950872

15. Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S.: Blockchain technology applications in healthcare: an overview. Int. J. Intell. Networks **2**, 130–139 (2021). https://doi.org/10.1016/J.IJIN.2021.09.005
16. Wood, G.: Ethereum: A Secure Decentralised Generalised Transaction Ledger (2014)
17. Szabo, N.: Smart Contracts : Building Blocks for Digital Markets (2018)
18. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
19. Omolara, A.E., Jantan, A.: Modified honey encryption scheme for encoding natural language message. Int. J. Electric. Comput. Eng. **9**(3), 1871–1878 (2019). https://doi.org/10.11591/IJECE.V9I3.PP1871-1878
20. Zhang, C., Wu, C., Wang, X.: Overview of blockchain consensus mechanism. ACM International Conference Proceeding Series, pp. 7–12 (2020). https://doi.org/10.1145/3404512.3404522
21. Ma, G., Ge, C., Zhou, L.: Achieving reliable timestamp in the bitcoin platform. Peer Peer Netw. Appl. **13**(6), 2251–2259 (2020). https://doi.org/10.1007/S12083-020-00905-6/METRICS
22. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E.: Enabling localised Peer-to-Peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. Industr. Inform. **13**(6), 3154–3164 (2017). https://doi.org/10.1109/TII.2017.2709784
23. Tosh, D., Shetty, S., Foytik, P., Kamhoua, C., Njilla, L.: CloudPoS: a proof-of-stake consensus design for blockchain integrated cloud. IEEE International Conference on Cloud Computing, CLOUD, vol. 2018-July, pp. 302–309 (2018). https://doi.org/10.1109/CLOUD.2018.00045