

Cryptospatial Blockchain Sharia Hotel Based on Practical Byzantine Fault Tolerance

Moch. Ainur Rahman Suryana, Achmad Teguh Wibowo, Andik Izuddin, Faris Muslihul Amin, Agustinus Bimo Gumelar, and MY Teguh Sulistyono

Abstract — This research develops an application based on android that uses four interconnected nodes in a network with the Practical Byzantine fault tolerance (PBFT) blockchain method to value object geospatial retrieval. First, this application uses two types of users, general users and surveyors. Second, a surveyor location is validated within a radius of fifty meters from the central point of assets location using midpoint circle validation. Third, PBFT is used to access and validate and guarantee consistency by data using JSON-DIFF algorithm.

Keywords — Blockchain PBFT, Geospatial Retrieval, JSON-DIFF Algorithm. Midpoint Circle Validation.

I. INTRODUCTION

NOWADAYS, cybercrime is intensely dangerous in the digital world [1]. Along with technological developments, many cybercrimes by evolution become more complicated so they cannot be trackable [2]. For example, penetration techniques are developing using existing vulnerabilities in third-party software to obtain valuable data from another system. Another attack technique is the ransomware virus, its ability to scramble system files and replicate data quickly on computers using the same network [3]. Therefore, it is necessary to solve fundamental aspects of data security and integrity between data [4].

The utilization of technology can solve the problem of security and integrity by data, such as blockchain technology. This technology is a new method to enhance security and integrity by data [5]. Blockchain combines the advantages of peer-to-peer networks and cryptography

Paper received January 20, 2021; revised March 18; accepted March 20, 2021. Date of publication July 31, 2021. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Miroslav Lutovac.

Moch. Ainur Rahman Suryana is with the Faculty of Science and Technology, UIN Sunan Ampel, Surabaya, Indonesia (phone: 0822-32510444; e mail: h76216060@uinsby.ac.id).

Achmad Teguh Wibowo, S.Kom, M.T, is with the Faculty of Science and Technology, UIN Sunan Ampel, Surabaya, Indonesia; (phone: 0811-30975699, e mail: atw@uinsby.ac.id).

Muhammad Andik Izuddin, MT is with the Faculty of Science and Technology, UIN Sunan Ampel, Surabaya, Indonesia; (phone: 0856-3297-556, e-mail: andik@uinsby.ac.id).

Faris Muslihul Amin, M.Kom is with the Faculty of Science and Technology, UIN Sunan Ampel, Surabaya, Indonesia; (phone: 0811-3257-959, email: faris@uinsby.ac.id).

Agustinus Bimo Gumelar, M.T is with the Faculty of Computer Science, Universitas Narotama, Indonesia; (phone: 0818-528-828, email: bimogumelar@ieec.org).

MY Teguh Sulistyono, M.Kom is with the Faculty of Computer Science, Universitas Dian Nuswantoro, Indonesia; (phone: 0822-2758-7676, email: teguh.sulistyono@dsn.dinus.ac.id).

to ensure data integrity connected in the blockchain network [6]. In cryptocurrency (bitcoin), blockchain is the largest and most popular technology for distributed digital transactions [7]. Blockchain technology uses a distributed database and transaction records shared with members in a network [5]. Rule of blockchain must be following an agreed consensus for every transaction in a distributed database network to reduce fraud activity [8].

Success of blockchain technology sparked a lot of attention and increased interest in various industries [9], such as in the tourism industry. This industry can use blockchain for geospatial retrieval to mapping dan sharing information, such as coordinate, name, photo, etc. This technology is called Crypto Spatial Coordinate (CSC); CSC uses a record time and validates locations [10]. This data is used in geographic information retrieval (GIR) [11].

To validate the data sent on the blockchain network the Midpoint Circle algorithm is used. This algorithm is an efficient algorithm to validate users' location by determining the radius and center value by real location [12]. Midpoint circle algorithm is combined with the PBFT algorithm, where PBFT is used to maintain data consistency between connected blockchain nodes. Meanwhile, the midpoint circle is used to validate the user's coordinates adjusted to the coordinates of the location assets.

The city of Surabaya has implemented a smart city (SC) System [13]. SC concept is an urban development that uses an information system (IS) perspective by collecting, analyzing, and exchanging information based on a supportive technology [14]. In Surabaya, there are several sharia hotels scattered in strategic locations and supported by many Muslim tourist visitors. However, sharia hotels are less familiar with tourists, so it is necessary to develop an application to display information from CSC blockchain-based sharia hotels to support the city's smart city system. This system also uses JavaScript Object Notation (JSON) as data validity. JSON is a JavaScript-based object format used in various programming languages (PHP, JS, C #, etc.). JSON is easier to use because it has lower power consumption when building the application [15].

This research develops a geospatial retrieval application to mapping Sharia hotels using the Practical Byzantine Fault Tolerance Blockchain (PBFT). This system is using the PBFT blockchain with a fault-tolerance value of 33%. This application was developed using React Native [16]. There are two types of users in this system, general users

and surveyor users. A surveyor could input sharia hotel assets through the application if the information were successfully entered when the real surveyor's location inside the midpoint radius approximately 50m from midpoint has been determined and has a value of fault tolerance less than 33% or vice versa. Information that is saved in a blockchain network is a JSON-DIFF [17], and contains coordinate, address, photo, and phone number of Sharia hotel, respectively. JSON-DIFF is used to compare the private hash value of each connected node, taking into account the fault tolerance value on the PBFT blockchain. If the value is true, it can be accessed or vice versa.

This paper is arranged as follows: Section I describes a combination of geospatial and blockchain to sharia hotel mapping. Section II explains the methodology. A literature study contains a mapping of Sharia hotels using GIR, PBFT blockchain, and midpoint circle validations are shown in Section III. Result and discussion in this research are shown in Section IV. Finally, a conclusion in this research and a suggestion for future directions are shown in section V.

II. METHODOLOGY

In this research, there are seven processes. The first is conducting a literature study on previous research on sharia hotels, PBFT blockchain, GIR, midpoint validation, and JSON. The second is to analyze the needs of a government city of Surabaya about Sharia hotels. The result of this process is to get the required data in this research. The third is to develop a digital map application using google maps [18]. The fourth is to enter the coordinate location, name, address, and phone number of the Sharia hotel. In the fifth, before adding assets to the blockchain, assets will be validated using the midpoint circle algorithm for smart contracts and PBFT for the consensus process. If the previous process is true, then the blockchain will create a new block in the blockchain network. The sixth blockchain will validate the private hash on each block using JSON-DIFF to access data. The seventh - an evaluation of the system that has been developed. Fig. 1 shows the experiment design of this research.

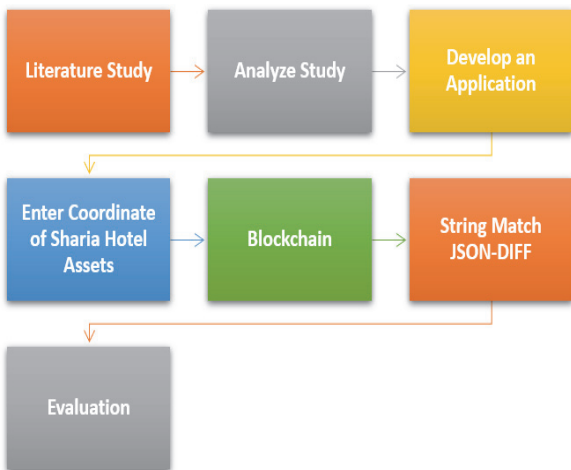


Fig. 1. Sharia Hotels with Blockchain Experiment Design.

III. LITERATURE STUDY

A. Sharia Hotel

Halal tourism is a tourist spot that considers Islamic law (sharia) as a basis for introducing products to Muslim customers [6]. Such as Sharia hotels, the Sharia hotel business is a robust business to attract Muslim tourists. By looking at the number of Muslim Indonesians, the Sharia hotel business will become a popular business in Indonesia [19].

B. Blockchain

Blockchain technology is a distributed database and records transactions shared with users who are members of the blockchain network [5]. Every transaction that occurs must be the agreed consensus.

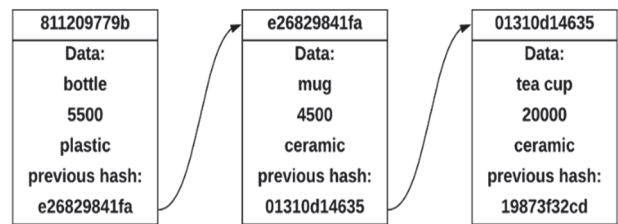


Fig. 2. Illustration of Blockchain.

Fig. 2 shows that each block on the blockchain network has three essential components: data, the previous hash of the last block, and the next hash.

C. Geographic Information Retrieval (GIR)

Geographic information retrieval is a system that takes place names, geographic spatial values [20]. In this research, GIR is used to develop a mapping application using Google Maps [18]. This process will generate information about coordinates, address, photo, and phone number of the Sharia hotels.

D. Practical Byzantine Fault Tolerance (PBFT)

PBFT is a blockchain protocol mechanism that uses a simple algorithm but has high practicality with distributed database systems [21]. PBFT blockchain has five stages: request, pre-prepare, prepare, commit, and reply [22]. In this research, the PBFT blockchain uses four virtual containers using dockers [23] with a specification of 8GB RAM and the Ubuntu 18.04 operating system. Docker is built for developing, delivering, and running applications. Docker allows you to separate applications from your infrastructure so you can deliver software quickly [23]. Fig. 3 shows how the process consensus PBFT blockchain works.

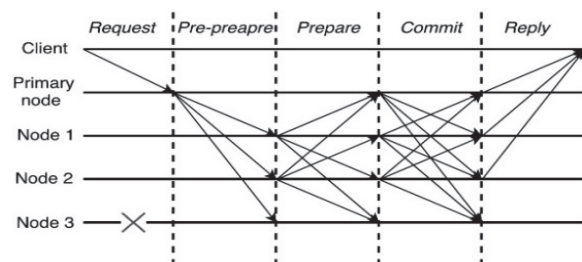


Fig. 3 Process of the consensus PBFT blockchain [22].

The equation of the PBFT is:

$$3f + 1 \quad (1)$$

where f is fault tolerance.

E. Midpoint Circle Validation Algorithm

The midpoint circle validation algorithm is an efficient conventional algorithm for drawing circles [20]. The radius is determined by the value r , and the coordinates of the position are (x_c, y_c) . In this research, the radius used to determine the midpoint of the object is 50 m. If the user is inside a radius, it is true or vice versa. The equation of this algorithm is:

$$f(x, y) = (x - x_c)^2 + (y - y_c)^2 - r^2. \quad (2)$$

where:

$f(x, y)$ - circular equation,

x - latitude,

y - longitude

r - radius

F. JavaScript Object Notation (JSON)

JSON is a JavaScript-based object format used in various programming languages (PHP, JS, C #, etc.). JSON is easier to use because it has lower power consumption when building the application [15]. JSON has two ways of writing, namely the JSON object and JSON array. JSON objects usually start with "{" and end with "}," and JSON array begins with "[" and ends with "]" [17]. In this research, JSON compares each block's private-key values in the blockchain network by using JSON-DIFF.

IV. RESULTS AND DISCUSSION

After conducting a literature study, the design of system workflow was obtained and is shown in the use case diagram and class diagram.

A. Use Case Diagram

They are two actors in the use case diagram. First, general users can only use the application that has been developed. Second, surveyor users can input data containing coordinate, name, photo, and phone number if the surveyor has been registered and validated real coordinate inside radius of Sharia hotels location predetermined. Use case diagram in this research shown in Fig. 4.

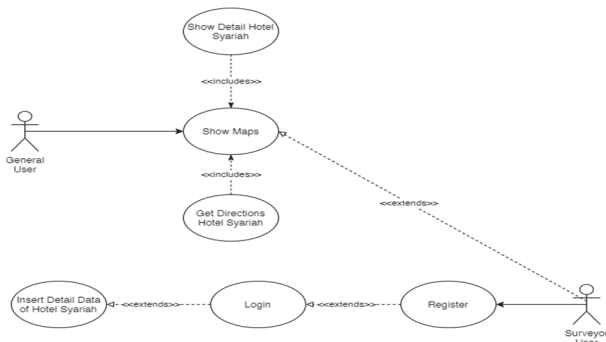


Fig. 4. Use Case Diagram in this research.

B. Class Diagram

There are 8 classes contained in the class diagram in this

research. The class is divided into 2 parts (front-end and back-end). In the front-end, there are class names Login and FetchAPI, while in the back-end, there are class names CenterController, UserController, BlockchainController, and DecryptController. Class diagram in this research shown in Fig. 5.

C. Implementation

The results of the UI design implementation that has been developed, are shown in Fig. 6.

Fig. 6. A displays the registration page for new users who wish to register as surveyors. Fig. 6.B displays the login page by entering the username and password. Figure 6.C displays a form page for encrypting new assets into the blockchain. In this menu, some information about sharia hotels is displayed in Fig. 6.D. Fig. 6.E shows some sharia hotel markers that have been decrypted.

D. Blockchain

Testing of the PBFT algorithm is latency comparison when encrypting and decrypting using 3G and 4G networks. The results of testing encrypt and decrypt processing are shown in Fig. 7 and Fig. 8, respectively.

Fig. 7. shows that the 4G is faster than the 3G; this can occur because the technology 4G enhance from the 3G network. The following evaluation is to know performed the mobile device's speed to decrypt data in the blockchain network, where the 4G network is faster than the 3G when used to send replied messages to the client using all the nodes that have succeeded a consensus process, the result of this evaluation is shown in Fig. 8. The whole evaluation process was carried out 100 times to get the average time shown in Table 1.

TABLE 1: AVERAGE TIME IN ALL NETWORK LATENCY.

<i>Evaluation</i>	<i>3G</i>	<i>4G</i>
Encryption	2.047s	0.617s
Decryption	0.414s	0.297s

Table 1 shows that 4G networks have an encryption execution time faster than the 3G networks amounting to 107%, while when decrypting 4G network faster than 3G network amounting to 33%.

The next evaluation is the midpoint circle validation. This test validates the user's position within 50m inside the radius of Sharia hotel from the center point predetermined. Table 2 shows the results of the point validation test carried out 100 times.

TABLE 2: MIDPOINT CIRCLE VALIDATION.

<i>Distance</i>	<i>Expected</i>		<i>Fact</i>	
	<i>True</i>	<i>False</i>	<i>True</i>	<i>False</i>
> 50m	0	100	0	100
< 50m	100	0	100	0

Table 2 shows that the percentage of success in this research reaches 100%. Expected and obtained values are the same. And last evaluation of this research is to evaluate the PBFT blockchain with four nodes using JSON-DIFF. The fault tolerance value used on the PBFT blockchain is 33% [22]. Table 3 shows the results of the evaluation.

TABLE 3: JSON-DIFF EVALUATION.

No.	Primary	Node 1	Node 2	Node 3	Expected	Fact
1	True	True	True	True	Running	OK
2	True	True	True	False	Running	OK
3	True	True	False	False	Failed	OK
4	True	False	False	False	Failed	OK
5	False	True	True	True	Failed	OK
6	False	True	True	False	Failed	OK
7	False	True	False	False	Failed	OK
8	False	False	False	False	Failed	OK

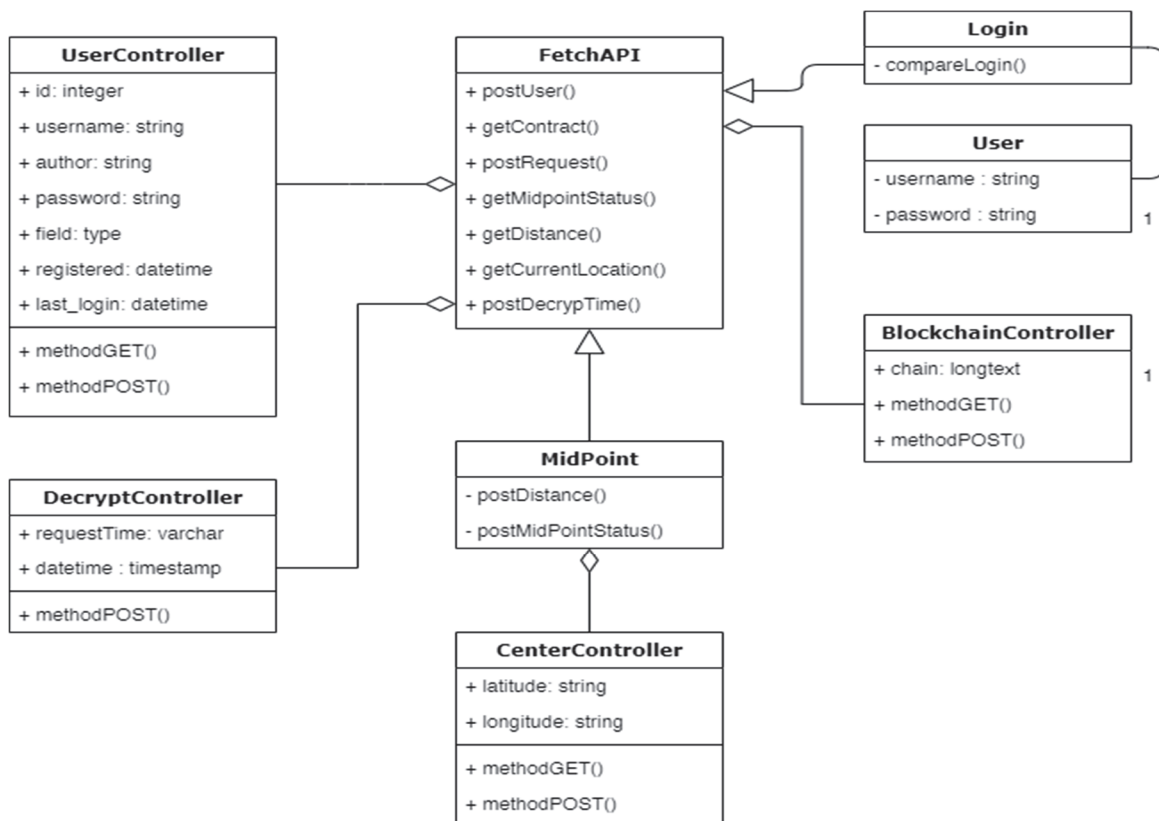


Fig. 5. Class Diagram in this research.

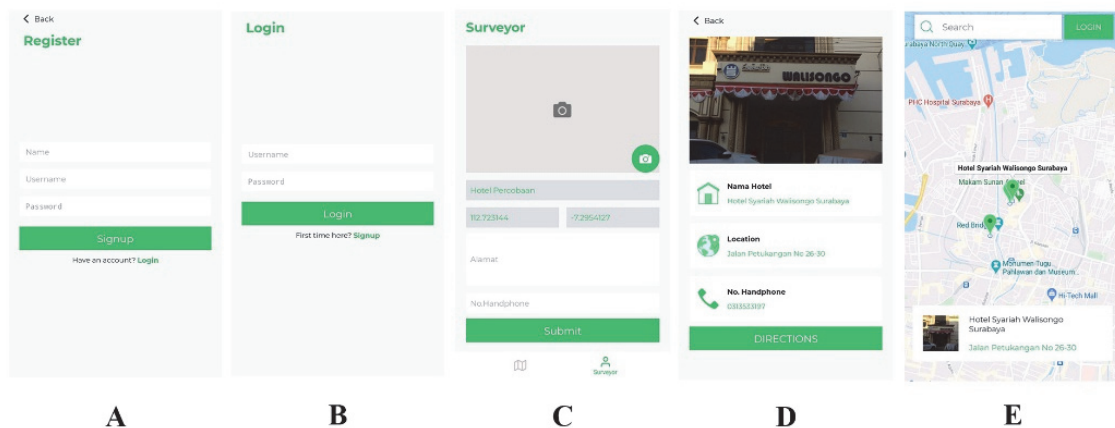


Fig. 6. (A) Register page, (B) Login Page, (C) The GIR for encrypted blockchain, (D) Hotel Sharia Assets, (E) The GIR for decrypted blockchain.

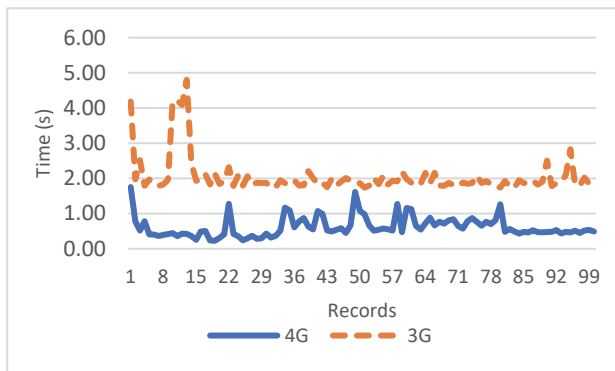


Fig. 7. Comparison of 3G and 4G network encryption latency.

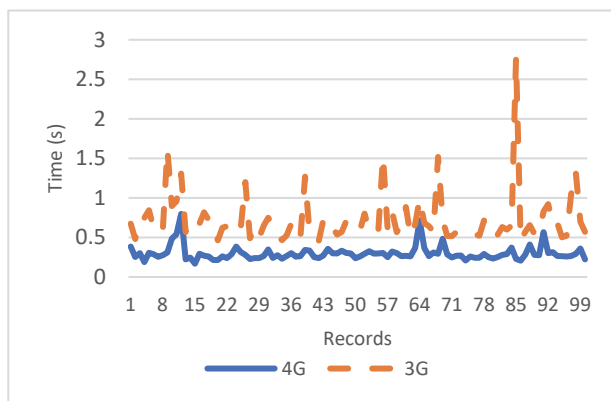


Fig. 8. Comparison of 3G and 4G network decryption latency.

V. CONCLUSIONS AND FUTURE DIRECTIONS

This research aims to develop a mapping application using GIR, React Native, NodeJS, and Google Maps as digital map services. The application runs on Android version 9 using the Snapdragon 625 chipset and 4GB of memory. The blockchain used is the CSC-based PBFT blockchain. This research evaluates the execution time of the PBFT blockchain when encrypting and decrypting 3G and 4G networks. The evaluation of 4G networks is faster than 3G, amounting to 107% to encrypt and 33% to decrypt data from the blockchain network.

This application has been presented at the Ministry of Religious Affairs Indonesia in the city of Surabaya. They are very enthusiastic about developing applications and providing data on Sharia hotel destinations in Surabaya. This research tested using the midpoint circle validation algorithm as surveyor real location validation. The scenario results show that validating each node's private key using JSON-DIFF is similar to fact and expected, so that percentage of success amounting to 100%.

For the future direction, it is advisable to add nodes connected to the blockchain and add validation algorithms such as the Rabin Karp Algorithm and many more. Furthermore, the system for development is not limited to using android only (iOS, Web-Based, and others).

REFERENCES

- [1] D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-Attack Penetration Test and Vulnerability Analysis," *Int. J. Online Biomed. Eng.*, vol. 13, no. 1, pp. 125–132, 2017.
- [2] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *7th Int. Conf. Financ. Criminol.*, 2015, vol. 28, no. April, pp. 24–31, 2015.
- [3] A. M. Gamundani and L. M. Nekare, "A Review of New Trends in Cyber Attacks: A Zoom into Distributed Database Systems," *2018 IST-Africa Week Conference (IST-Africa)*, 2018.
- [4] G. Sivathanu, C. P. Wright, and E. Zadok, "Ensuring Data Integrity in Storage: Techniques and Applications," *Proc. 2005 ACM Work. Storage Secur. Surviv. - StorageSS'05.*, pp. 26–36, 2005.
- [5] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Comput. Sci.*, vol. 123, pp. 116–121, 2018.
- [6] M. Battour and M. N. Ismail, "Halal tourism: Concepts, practises, challenges and future," *Tour. Manag. Perspect.*, vol. 19, pp. 150–154, 2016.
- [7] J. Ghosh, "The Blockchain: Opportunities for Research in Information Systems and Information Technology," *J. Glob. Inf. Technol. Manag.*, vol. 22, no. 4, pp. 235–242, 2019.
- [8] A. T. Wibowo, M. Hariadi, M. Y. T. Sulistyono, M. Khusnu Milad, E. I. Rhofita and A. Bimo Gumelar, "Mapping of Tourism Destinations by GIS-Blockchain RPCA based on PNPOLY Algorithm," *2020 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2020, pp. 412-416.
- [9] I. Önder, and H. Treiblmaier, "Blockchain and tourism: Three research propositions" *Ann. Tour. Res.*, vol. 72, pp. 180-182, September 2018.
- [10] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare," *Int. J. Health Geogr.*, vol. 17, 25, 2018.
- [11] C. B. Jones and R. S. Purves, "Geographical information retrieval," *Int. J. Geogr. Inf. Sci.*, vol. 22, no. 3, pp. 219-228, March 2008.
- [12] B. V. Lakshmi and V. Mohan, "Plant Leaf Image Detection Method Using a Midpoint Circle Algorithm for Shape-Based Feature Extraction," *J. Mod. Appl. Stat. Methods*, vol. 16, no. 1, pp. 461–480, 2017.
- [13] BPS-Statistics of Surabaya Municipality, Kota Surabaya Dalam Angka, 1st ed., vol. 1. Surabaya: CV. Azka Putra Pratama, 2018.
- [14] A. M. Shahat Osman and A. Elragal, "Smart Cities and Big Data Analytics: A Data-Driven Decision Making Use Case," *Smart Cities*, vol. 4, no. 1, pp. 286–313, 2021.
- [15] A. R. Breje, R. Györödi, C. Györödi, D. Zmaranda, and G. Pecherle, "Comparative Study of Data Sending Methods for XML and JSON Models," *International Journal of Advanced Computer Science and Applications*, vol. 9 no. 12, 2018.
- [16] S. Bershadskiy and C. Villa, *React Native Cookbook*. 2016.
- [17] M. K. Yusof and M. Man, "Efficiency of JSON for Data Retrieval in Big Data," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 7, no. 1, pp. 250–262, July 2017.
- [18] Google. Inc, "Google Maps Platform Documentation." [Online]. Available: <https://developers.google.com/maps/documentation/>. [Accessed: 17-Mar-2021].
- [19] M. Mujahidin, "Sharia hotels in Indonesia: Concept and potential analysis," *Munich Pers. RePEc Arch.*, no. 90819, 2018.
- [20] Ross S. Purves; Paul Clough; Christopher B. Jones; Mark H. Hall; Vanessa Murdock, *Geographic Information Retrieval: Progress and Challenges in Spatial Search of Text*. Now Foundations and Trends, 2018.
- [21] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *Proc. Symp. Oper. Syst. Des. Implement.*, no. February, pp. 1–14, 1999.
- [22] S. Zhang and J. H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no.2 pp. 93-97, June 2020.
- [23] Docker, "Docker Documentation." [Online]. Available: <https://docs.docker.com/get-started/overview/>. [Accessed: 17-Mar-2021].