Achmad Teguh Wibowo - MY Teguh Sulistyono - Mochamad Hariadi

CRYPTOSPATIAL COORDINATE USING THE RPCA BASED ON A POINT IN POLYGON TEST FOR CULTURAL HERITAGE TOURISM

This research was aimed to enhance the cryptospatial with geospatial blockchain based on a point in polygon test. Ripple Protocol Consensus Algorithm (RPCA) was used for developing a blockchain. The steps taken include: (1) Data from the surveyors were entered using application connected to the transaction set; (2) The transaction set sent data to the transaction proposal; (3) The transaction proposal will distribute to every connected validating of nodes for executing the smart contract with the point in a polygon test method; (4) If the process succeeded with the maximum fault tolerance of 20%, then the node records a new chain to the ledger. This method is faster than Practical Byzantine Fault Tolerance (PBFT) blockchain for approximately 26% to add a new chain in the ledger and for 52% to decrypt the blockchain with a mobile device. The result of this process is a cryptospatial coordinate for the cultural heritage tourism.

Keywords: *cryptospatial coordinate, cultural heritage tourism, RPCA, point in polygon test*

1 Introduction

Blockchain has become a disruptive innovation for many aspects of technology, business and governance [1]. Nowadays, the government, companies, and organizations are started to develop this technology to be applied to the public [2]. How blockchain works are how many nodes connected in a distributed network could maintain consensus and this network to adopt of hash based Proof-of-Work (PoW) algorithm [3].

This technology combines the advantages of peer-to-peer networks and cryptography to ensure the data validity because an entity connected in a blockchain network cannot change the data that is approved unless it involves all connected in a blockchain [4]. Besides, blockchain can ensure the correctness of recorded transactions over time. This feature supports transaction security from all the entities that do not trust each other.

Besides used for cryptocurrency, the blockchain can be implemented in the tourism industry [5]. This industry has explored to offer more integrated services so that tourists get a holistic experience [6]. Combining the blockchain and geospatial retrieval could be used in the tourism sector because majority of information always contain the spatial data on earth that requires specific expertise to handle geospatial data [7]. This technology is called Crypto Spatial Coordinate (CSC), which is recorded of data entry within a particular time, validate related to location, and specific mapping objects in temporal sequences [8].

Data from The Ministry of Tourism of the Republic of Indonesia recorded tourist visits in 2019 reached 1,330,288, [9]. The City of Surabaya is one of the popular tourist destinations. This city has a long history so that many cultural heritages such as buildings, museums, hotels and others [10]. Nowadays, Surabaya has implemented the smart city technology. However, the tourism sector has not yet implemented that technology, such as providing route navigation to cultural heritage locations and utilizing the blockchain as a CSC for the smart city implementation.

Based on the previous explanation, this research discusses the CSC used SHA256 encryption for headers and AES encryption for content added to the blockchain network. The Ripple Protocol Consensus Algorithm (RPCA) used to provide maximum fault tolerance of 20% [11] using five computers. The fault tolerance, obtained from the polygon query algorithm process [12], is based on point in polygon test [13] to detect the validity of the data entered.

2 Cryptospatial coordinate

A good example of cryptospatial coordinate, using the blockchain, is a FOAM [14], because this product requires proof of location associated, an immutable geospatial context that regular blockchain lacks and many more, [8].

In this research, development of the geospatial blockchain used Google Maps Service [15]. This process produced data latitude and longitude coordinates based on location, address, photo, and detail information. This data would be processed, using the AES encryption, required a private key and public key to read the data. The header of

Achmad Teguh Wibowo[1,2], MY Teguh Sulistyono[1,3], Mochamad Hariadi[1,*]
[1]Department of Electrical Engineering, Faculty of Intelligent Electrical and Informatics Technology (ELECTICS), Sepuluh Nopember Institute of Technology, Surabaya, Indonesia
[2]Faculty of Science and Technology, UIN Sunan Ampel Surabaya, Indonesia
[3]Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia
*E-mail of corresponding author: mochar@ee.its.ac.id

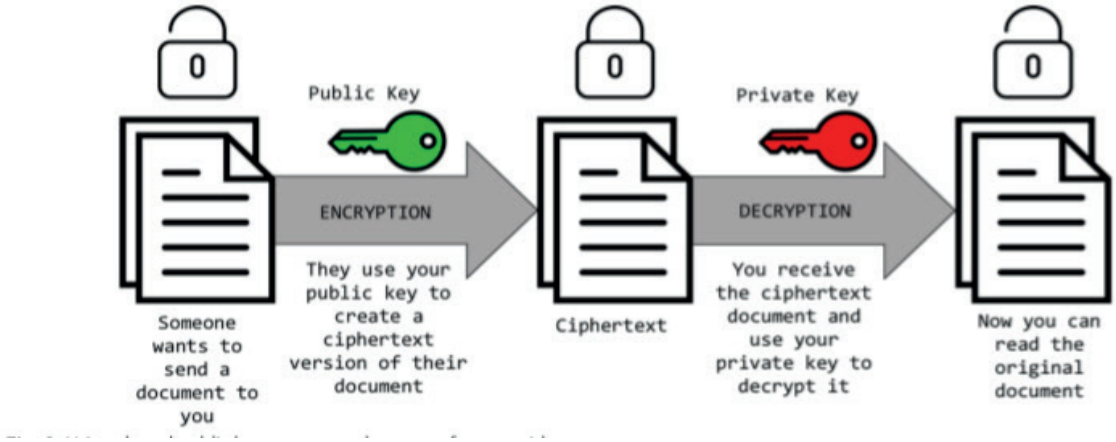

Figure 1 *Process encrypts the data using a private key [8]*

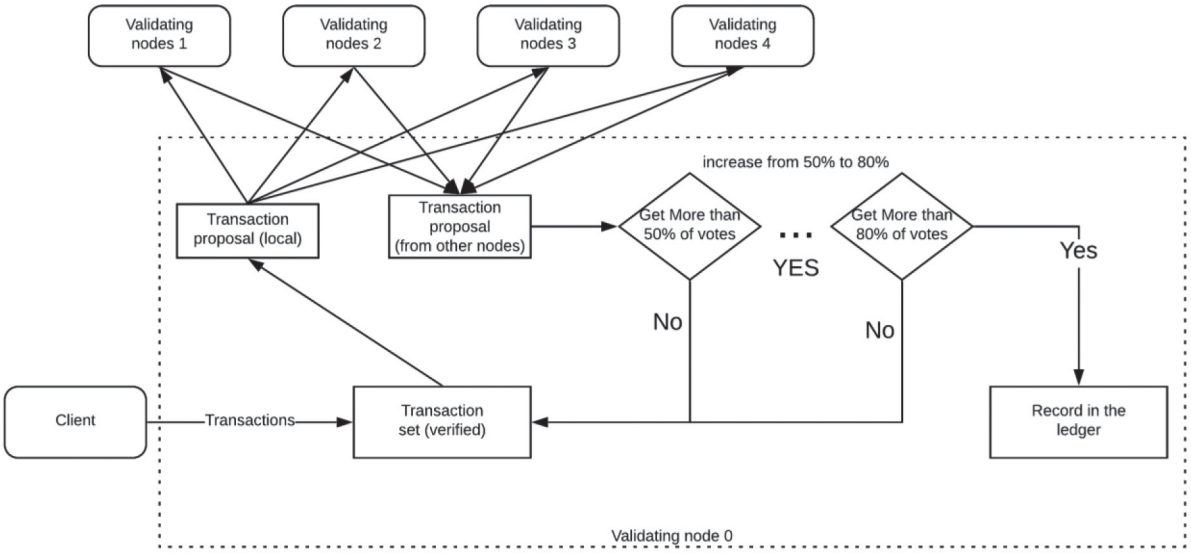

Figure 2 *Process of the consensus in the Ripple algorithm [16]*

Table 1 *Comparison of the main consensus permissioned blockchain*

Property	RPCA	PBFT
Type	Absolute-finality	Absolute-finality
Fault Tolerance	20%	33%
Power Consumption	Negligible	Negligible
Scalability	Good	Bad
Application	Permissioned	Permissioned

the blockchain was processed using SHA256 for validated data. Figure 1 explains encrypted data using a private key.

3 Ripple protocol consensus algorithm (RPCA)

Ripple does not use the PoW or Proof-of-Stake (PoS) mechanism to validate transactions because Ripple uses a consensus protocol with its specifications. This algorithm runs on per-missioned blockchain, unlike Bitcoin and Ethereum [16]. The RPCA algorithm is applied every few seconds by all the nodes to guarantee the transaction validity. The consensus process in Ripple validated by the node owned. This node called Unique Node List (UNL) [11]. Equation of the RPCA is:

$$F \leq (n-1)/5\,, \tag{1}$$

and the probability of correctness, given by p^*, is:

$$p^* = \sum_{i=0}^{\left(\frac{n-1}{5}\right)} \binom{n}{i} p_c^i (1-p_c)^{n-1}\,, \tag{2}$$

The pseudocode of the RPCA is shown:

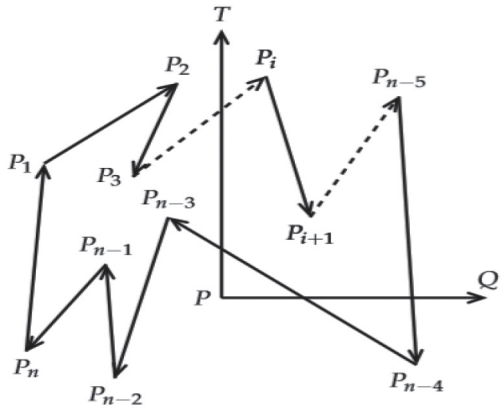

Figure 3 *Crossing Number Algorithm [19]*

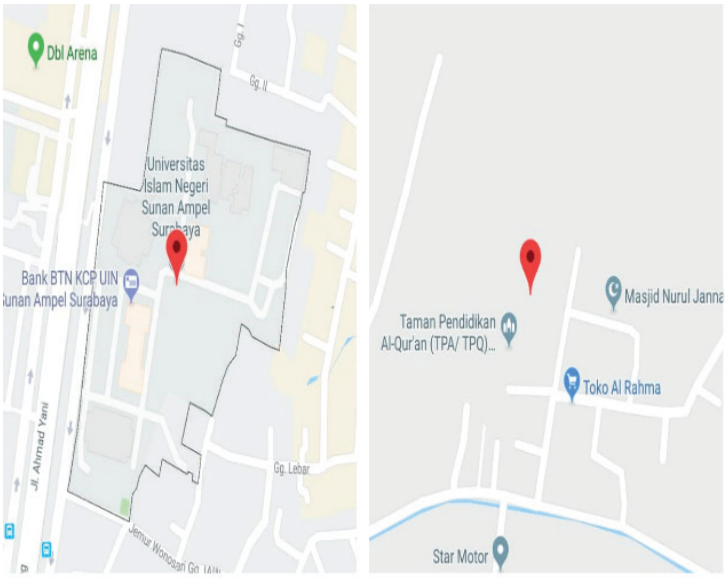

Figure 4 *(a) True condition while coordinate is inside the polygon area a predetermined, (b) False condition while coordinate is inside the polygon area a predetermined*

a) Each server processes a valid transaction and converts it to a transaction set;
b) The server sends a set of transactions to all the validation nodes to carry out a consensus process;
c) If the node produces true, then the transaction is delivered to the next transaction proposal, otherwise it will be discarded or inserted into the candidate ledger;
d) If the previous process gets a maximum error of 20%, then the transaction is
e) Recorded in a ledger, otherwise it will be discarded.

Figure 2 shows the process of the consensus in the Ripple algorithm and comparison of the main consensus protocol permissioned blockchain [16] is shown in Table 1.

4 Point in polygon test

The point in Polygon Test in this research uses the crossing number method. This method is a popular tool in drawing and visualization [17]. This research used the crossing number to calculate the ray line passing through the edge boundary polygon from point P. If the intersection number is even, then the point is outside the polygon area and vice versa, [18]. Figure 3 shows the crossing number algorithm.

This method is based on Jordan Curve Theorem [20]. This theorem explains a line repetition that does not intersect an object, separated into two components [21]. Equation of The Jordan Curve Theorem is:

$$C = \{(x,y); x^2 + y^2 = 1\}. \tag{3}$$

To enhance the crossing number the point in Polygon Test Test was used because this method runs a semi-infinite ray horizontal (increasing x, fixed y) from point P, and counting many boundary edges [18]. Equation of this method is:

$$f = \sum_{x=0,y=0}^{n,m} (y - y_m)(x_n - x_m) > \\ > (y_n - y_m)(x - x_m). \tag{4}$$

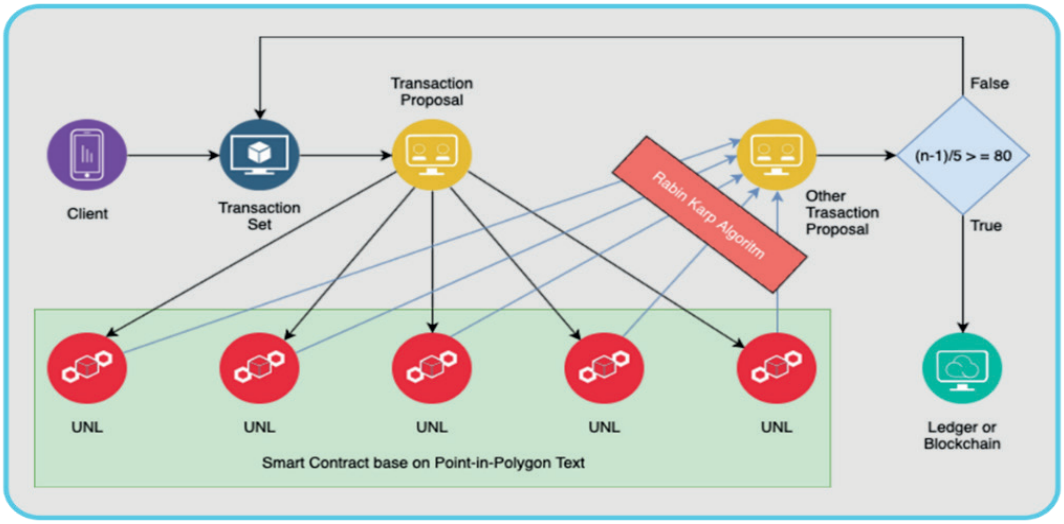

Figure 5 *Design of the RPCA in This Research*

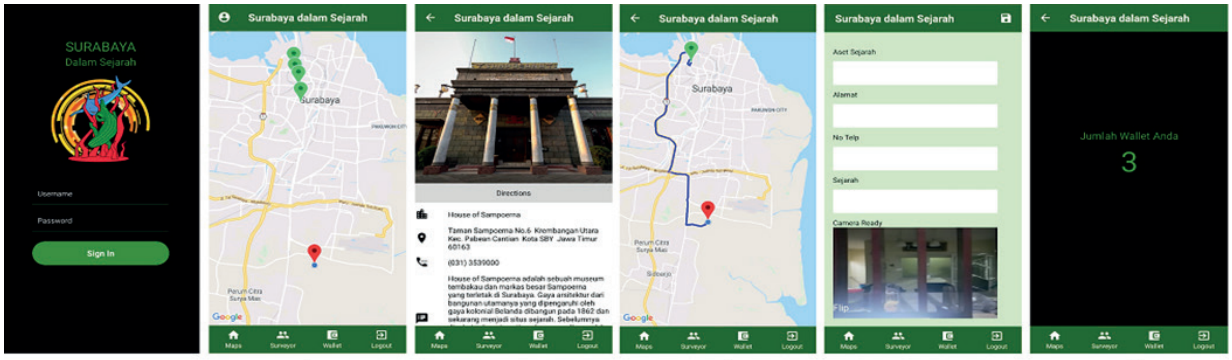

Figure 6 *(a) Login Form, (b) CSC of the decrypted blockchain, (c) The cultural heritage asset of the decrypted blockchain, (d) Form navigate to the cultural heritage asset, (e) Form input cultural heritage asset for encrypted to the blockchain, (f) Wallet balance for the surveyors*

An illustration of the point-in-polygon test method is shown in Figure 4.

5 Design

The experiment in a laboratory consisted of 9 computers and one mobile device. Specifications of 9 computers used consist of 4 GB of memory, I3-4150 CPU and Intel HD graphics card 4400. All the computers used Windows 10 platforms. Mobile devices used SOC Snapdragon 660, 4 GB of memory and Android 8 as the operating system. Figure 5 shows design of the RPCA for this research.

Figure 5 explains the process of this research. (1) Surveyor requests to send data of geospatial retrieval to be processed into a transaction set. (2) This server managed data and would it be sent to the transaction proposal. (3) This process would send data to the UNL that has been developed. (4) The UNL conducted a smart contract with the Point-in-Polygon Test method. The result of this process is true or false, if the result is right, then the Rabin Karp method validates the string with equation $f \leq (n-1)/5$. If the result of the vote UNL is ≥ 80%, then the system would create a new block into the ledger.

6 Implementation

The product of this research is an application based on mobile technology [22]. This product is shown in Figure 6.

Figure 6(a) shows the login form and a user must be registered in the whitelist account to add a new chain and view the total balance of their wallet. Figure 6(b) shows the marker of the assets a cultural heritage into the map. This marker is obtained from the decrypted data using the AES decryption. This data is CSC, which is obtained from the RPCA process.

Figure 6(c) shows the results of the decrypted method from the blockchain. This data includes photos, addresses, telephone numbers, and coordinates used to navigate to the cultural heritage location, selected in the previous process.

Navigate menu shown in Figure 6(d), where this menu can help the tourist to go in the direction of a cultural heritage location using the mobile devices.

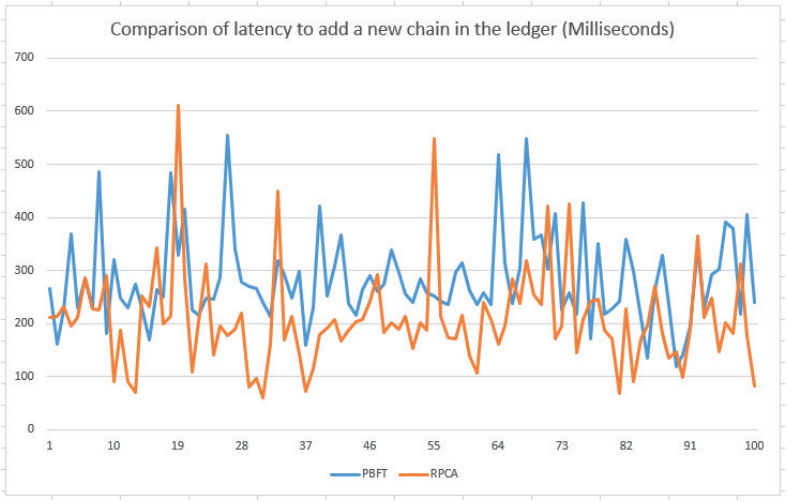

Figure 7 *Comparison of the latency RPCA and PBFT*

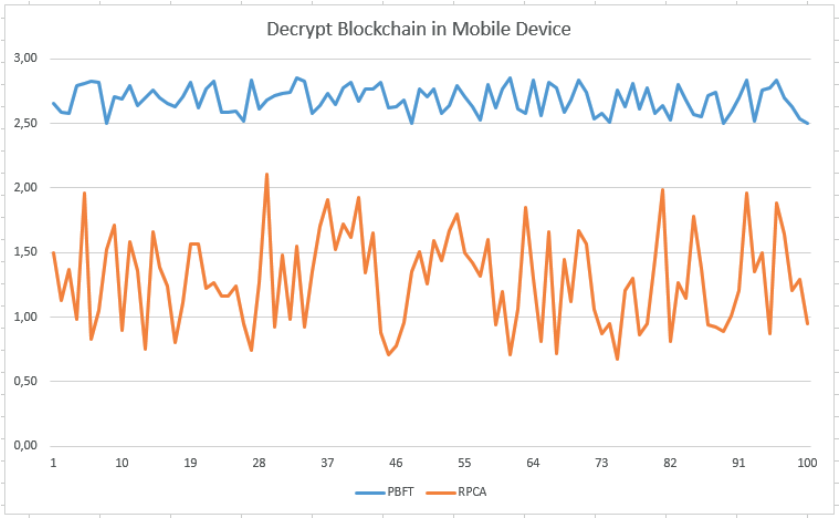

Figure 8 *Decrypt blockchain RPCA and PBFT in Mobile Device*

Table 2 *Average time in all evaluations*

Evaluation	RPCA	PBFT
Comparison of latency to add new chain	207.5626ms	282.2318ms
Decrypt blockchain in mobile device	1.29s	2.69s

Figure 6(e) shows the input form for the surveyor. This form consists of inputting a name, address, telephone and place description, photos and coordinates location of the cultural heritages. These coordinates are obtained by the location-based services from the surveyor's mobile device. Blockchain would validate coordinates sent by a surveyor, using a point-in-polygon test algorithm. If the coordinate is inside the polygon area, then value of the UNL server from consensus becomes true or vice versa. Figure 6(f) shows the wallet balance owned by the surveyor. This balance would be increased if input data by the surveyor is successfully validated by the UNL Server with a value ≥ 80% of fault tolerance, so that a new chain could be added to the ledger.

7 Evaluation

The first evaluation is presented in Figure 7. This evaluation shows the latency of the process to add a new chain in the ledger using the RPCA. This process output is compared to the PBFT method, using a similar specification computer. The PBFT method is used in a similar case. That research used five computers and one mobile device. One computer was used for the primary node and another computer was used for nodes to the smart contract process, the equation of this method is:

$$3f + 1\,, \tag{5}$$

where *f* is the number of fault tolerance obtained from the consensus process.

Figure 7 shows that the RPCA is faster than the PBFT; this can occur because the PBFT method emphasizes the consistency of data in each node. However, the RPCA has advantages over the PBFT, especially related to speed for the consensus process. The next evaluation was performed to know the speed of the mobile device to the decrypt blockchain shown in Figure 8.

Figure 8 shows that the RPCA is faster than the PBFT method, because the PBFT sent replied messages to the client using all the nodes that have succeeded in the consensus process. The whole evaluation was carried out for 100 times to get the average time shown in Table 2.

8 Conclusions and future direction

This research was limited to the city of Surabaya and used the mobile application based on the React Native that has been tested, a mobile device with specifications: SOC Snapdragon 660, 4 GB of memory and Android 8 as the operating system. Implementation blockchain based on RPCA for CSC has been developed.

The allowed blockchain methods, especially the RPCA and PBFT, were compared. The result of evaluation is that the RPCA method is faster than the PBFT, approximately for 26% to add a new chain in the ledge, because the PBFT method emphasizes the consistency of data in each node.

The next experiment was testing the speed of the mobile device to decrypt blockchain. The evaluation result shows the time required for a mobile device to decrypt the blockchain; the RPCA method is faster for 52% than the PBFT, because the PBFT method runs by sent-replied messages to the client, using all the nodes that have succeeded in the consensus process.

This application has been presented at the Government Surabaya City Tourism Office. They are enthusiastic about developing the app and are willing to provide data on tourism destinations, especially cultural heritage tourism, to be implemented in it. Besides that, they have suggested a collaboration with Ministry of the Religion of Republic of Indonesia to use this application for the halal tourism, since the halal tourism sector has become a trend, especially in Indonesia.

It is suggested to consider the fault tolerance for the appropriate application scenario, because the design of the main consensus protocol, especially the RPCA and PBFT, has advantages and weaknesses to implement in any case and the RPCA method was proposed wince it could be applied for the CSC, not only cryptocurrency.

For the future directions, a novel algorithm was developed, to implement this application that is a combination blockchain of the RPCA and PBFT, which is currently still in the development phase. Implementation of this application is not only limited to the tourism sector, but it can be implemented for other areas, such as health, education, endowments, and many more.

References

[1] DOGRU, T., MODY, M., LEONARDI, C. Blockchain technology and its implications for the hospitality industry. *Boston Hospitality Review*. 2018, **winter**, p. 1-12. ISSN 2326-0351.

[2] HEBERT, C., DI CERBO, F. Secure blockchain in the enterprise: a methodology. *Pervasive and Mobile Computing* [online]. 2019, **59**, p. 101038. ISSN 1574-1192. Available from: https://doi.org/10.1016/j.pmcj.2019.101038

[3] NAKAMOTO, S. *Bitcoin: a peer-to-peer electronic cash system* [online]. 2008. Available from: https://bitcoin.org/bitcoin.pdf

[4] AL-JAROODI, J., MOHAMED, N. Blockchain in industries: a survey. *IEEE Access* [online]. 2019, **7**, p. 36500-36515. eISSN 2169-3536. Available from: https://doi.org/10.1109/ACCESS.2019.2903554

[5] ONDER, I., TREIBLMAIER, H. Blockchain and tourism: three research propositions. *Annals of Tourism Research* [online]. 2018, **72**, p. 180-182. ISSN 0160-7383. Available from: https://doi.org/10.1016/j.annals.2018.03.005

[6] GRETZEL, U., SIGALA, M., XIANG, Z., KOO, C. Smart tourism: foundations and developments. *Electronic Markets* [online]. 2015, **25**(3), p. 179-188. ISSN 1019-6781, eISSN 1422-8890. Available from: https://doi.org/10.1007/s12525-015-0194-x

[7] PURVES, R. S., CLOUGH, P., JONES, C. B., HALL, M. H., MURDOCK, V. Geographic information retrieval: progress and challenges in spatial search of text. *Foundations and Trends in Information Retrieval* [online]. 2018, **12**(2-3), p. 164-318, 2018. ISSN 1554-0669, eISSN 1554-0677. Available from: http://dx.doi.org/10.1561/1500000034

[8] KAMEL BOULOS, M. N., WILSON, J. T., CLAUSON, K. A. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *International Journal of Health Geographics* [online]. 2018, **17**(1), p. 1-10. ISSN 1476-072X. Available from: https://doi.org/10.1186/s12942-018-0144-x

[9] Data on monthly foreign tourist visits in 2019 - Ministry of Tourism Republic of Indonesia [online] [accessed 2019-09-10]. 2019. Available from: http://www.kemenpar.go.id/post/data-kunjungan-wisatawan-mancanegara-bulanan-tahun-2019

[10] PUTRA, D. W. Identification of the sustainability of the old town area through the protection of cultural heritage buildings by the surabaya city government. *Jurnal Pengembangan Kota*. 2016, **4**(2), p. 139. ISSN 2337-7062, eISSN 2503-0361.

[11] SCHWARTZ, D., YOUNGS, N., BRITTO, A. *Analysis of the XRP ledger consensus protocol* [online] [accessed 2019-10-26]. Cornell University, 2018. Available from: https://arxiv.org/pdf/1802.07242

[12] KHATUN, F., SHARMA, P. Arbitrary polygon query handling algorithm on GIS based on three value logic- an approach. *International Journal of Computer Applications* [online]. 2016, **144**(1), p. 32-35. ISSN 0975-8887. Available from: https://doi.org/10.5120/ijca2016910090

[13] KUMAR, G. N., BANGI, M. An extension to winding number and point-in-polygon algorithm. *IFAC-Papers On Line* [online]. 2018, **51**(1), p. 548-553. ISSN 2405-8963. Available from: https://doi.org/10.1016/j.ifacol.2018.05.092

[14] CORP, F. *FOAM map* [online] [accessed 2019-08-17]. 2019. Available from: https://foam.space/

[15] Google maps platform documentation - Google. Inc [online] [accessed 2019-07-20]. Available from: https://developers.google.com/maps/documentation/

[16] ZHANG, S., LEE, J.-H. Analysis of the main consensus protocols of blockchain. *ICT Express* [online]. 2019, **2**, p. 1-5. ISSN 2405-9595. Available from: https://doi.org/10.1016/j.icte.2019.08.001

[17] SCHAEFER, M. The graph crossing number and its variants: a survey. *The Electronic Journal of Combinatorics* [online]. 2018, **1**, p. 1-113. ISSN 1077-8926. Available from: https://doi.org/10.37236/2713

[18] SUNDAY, D. *Inclusion of point in a polygon* [online]. **2011**. Available from: http://geomalgorithms.com/a03-_inclusion.html

[19] HAO, J., SUN, J., CHEN, Y., CAI, Q., TAN, L. Optimal reliable point-in-polygon test and differential coding boolean operations on polygons. *Symmetry* [online]. 2018, **10**(10), p. 1-26. eISSN 2073-8994. Available from: https://doi.org/10.3390/sym10100477

[20] PERLES, M. A., MARTINI, H., KUPITZ, Y. S. A Jordan-Brouwer separation theorem for polyhedral pseudomanifolds. *Discrete and Computational Geometry* [online]. 2009, **42**(2), p. 277-304. ISSN 0179-5376, eISSN 1432-0444. Available from: https://doi.org/10.1007/s00454-009-9192-0

[21] ROSS, F., ROSS, W. T. The Jordan curve theorem is non-trivial. *Journal of Mathematics and the Arts* [online]. 2011, **5**(4), p. 213-219. ISSN 1751-3472, eISSN 1751-3480. Available from: https://doi.org/10.1080/17513472.2011.634320

[22] BERSHADSKIY, S., VILLA, C. *React native cookbook take your react native application development to the next level with this large collection of recipes*. 1. ed. Birmingham: Packt, 2016. ISBN 978-1-78646-255-8.