I. J. Computer Network and Information Security, **2024, 5, 14-22**
Published Online on October 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.05.02

Blocking Fraud, Advertising, or Campaign-Related Calls with a Blockchain-based Mobile App

Remzi Gürfidan*
Isparta University of Applied Science, Yalvaç Vocational School of Technical Sciences, Computer Programming, Isparta, Turkey
E-mail: remzigujrfidan@isparta.edu.tr
ORCID iD: https://orcid.org/0000-0002-4899-2219
*Corresponding Author

Şerafettin Atmaca
Isparta University of Applied Science, Rectorate, Isparta, Turkey
E-mail: serafettinatmaca@isparta.edu.tr
ORCID iD: https://orcid.org/0000-0003-2407-1113

Received: 04 May 2023; Revised: 03 July 2023; Accepted: 12 October 2023; Published: 08 October 2024

Abstract: The use of a person's cell phone to commit fraud is known as cell phone fraud. Such scams are usually carried out through fake phone calls or text messages. The victim receives a call from a cell phone scammer, usually claiming to have an emergency or a legal problem. The purpose of the scam is usually to convince the victim to provide personal or financial information. This may include private information such as social security numbers, bank account details or credit card information. In addition, users are often subjected to unsolicited calls for marketing and information gathering initiatives such as campaigns, advertisements and surveys. In this study, a smartphone application built on the blockchain is created to stop these nuisance actions. Transaction times and performance tests have been rigorously performed according to the difficulty levels of the blockchain structure.

Index Terms: Blockchain, Blockchain Scalability, Mobile Fraud, Fraud Prevention.

1. Introduction

In recent years, the number of mobile phone users has been increasing at an incredible rate [1]. The increasing number of phone scams has become a major problem in all countries [2]. This method of fraud is when fraudsters try to trick victims over the phone in order to obtain money or personal information. Recent statistics on telephone fraud show an increase in this type of crime. However, these figures may differ in other countries and regions. The US Federal Trade Commission reports that in 2020, Americans lost around $1.9 billion to fraud. Most of this is attributed to losses to phone scammers. Data from the UK National Crime Agency shows that £68 million was lost to phone fraud in the UK in 2020. This is a 20% increase compared to the previous year. Data from the Australian Competition and Consumer Commission shows that phone fraud losses in Australia reached $48 million in 2020. This is a 23% increase compared to the previous year. The Canadian Anti-Fraud Center reported that phone fraud losses in Canada exceeded 74 million Canadian dollars in 2020. This figure was found to have increased by 65% compared to the previous year [3].

These figures show that phone fraud is a significant problem with a global impact. Therefore, it is crucial to be vigilant against phone fraud and take proactive measures to protect our privacy. These measures can include rejecting calls that seem suspicious, not transferring important information such as personal information, account numbers, etc. to the other party, being suspicious of requests that seem too good to be true, being cautious when a call from a government agency asks for money or personal information, and requesting an instant confirmation message from those who report that they are calling from official institutions or organizations.

In addition to the anxiety of fraud in the phone calls we make in daily life, we also receive calls from numbers with advertising, survey or campaign content. Some companies and institutions generally prefer corporate numbers for calls with such content. However, the number of calls with campaign and advertisement content, which has increased recently, negatively affects people's daily lives. People exposed to this situation block or do not answer calls from such corporate

numbers. In this reality-based scenario, companies and organizations prefer numbers reserved for personal use as an alternative to corporate numbers. This situation contains many negative situations.

Using advertising or campaign content to block unwanted calls is not practical or morally acceptable. It can even damage the reputation of the advertiser or campaign and be counterproductive. Firstly, using campaign or promotional content to block nuisance calls can be considered spamming, which is against various laws and regulations. Spamming can damage the reputation of an advertiser or campaign and may be subject to fines and penalties by law. If the recipient is prevented from receiving advertising or campaign calls, they may be offended and may develop negative associations with the brand or campaign. It may also be perceived as an intrusion into someone else's privacy, which can be upsetting and annoying. In addition to all these negativities, the person receiving the call will feel uneasy about being exposed to a scam. Users resort to methods such as using call blocking applications and joining national "call blocking" registries to avoid spam calls.

Blockchain is a powerful data security tool. A blockchain is a collection of linked blocks, each containing the previous block, a timestamp and a digital signature. Each block is added to the content of the previous block without any modification thanks to the date and digital signature. As a result, it is virtually impossible to alter or falsify the data recorded by the blockchain. Blockchain technology is widely used, especially in areas such as finance, where sensitive data needs to be held securely. Numerous other areas such as voting systems, smart contracts and health records also benefit from this technology.

Using a hashing algorithm designed specifically for cryptocurrencies like Bitcoin, blockchains execute a process called mining. To add new blocks to the blockchain, mining requires solving hash operations with specialized hardware and software. Blockchain mining activities are based on a level of difficulty [4]. The difficulty of blockchain mining activities is determined by this difficulty level. The security and efficiency of the blockchain depends on the difficulty level. In the blockchain, the mining activity and block duration are controlled by the difficulty level. This level takes into account the computational power required to solve the hash [5]. The total number of mining operations of the blockchain and the power of the hardware used determine this computational power. Depending on how fast and how difficult the mining operations are, the difficulty level is always changing. For example, as blockchain mining operations speed up, the difficulty level increases and hashes become more difficult to solve. On the other hand, as mining activities slow down, the difficulty level decreases and hashes become simpler. The difficulty level in the network is crucial for security and efficiency, as it determines the speed and difficulty of mining operations in the blockchain [6, 7].

In this study, a blockchain-based mobile application that can provide an alternative solution to the problems, blocking unwanted calls to cell phones, has been developed. The scalability of the developed blockchain structure has been rigorously tested and the transaction performances have been evaluated.

2. Related Works

Some preventive studies have been carried out to prevent fraud processes involving mobile applications and their content. In particular, the focus has been on issues such as increasing ad rankings [1], fraudulent ad placements, and preventing the spread of false information [8].

Machine learning methods are generally utilized in the developed systems and proposed models. Trained models reach their conclusions by taking into account certain feature inferences. Haider et al. conducted research on real-time fraud detection that aims to classify individuals as fraudulent or non-fraudulent. For the detection system, 21 different features were identified and an ensemble-based machine learning model was used. The model they developed achieved 97.95% classification success [9]. Another prevention method with a similar purpose using different methods was realized by Grosser and colleagues [10]. Mouawi et al. proposed a system for generating ad-related information and extracting features such as the proportion of unique IPs in the total number of clicks per publisher. They used three different classifiers to classify malicious publishers. All three classifiers gave very promising results. KNN seems to be the best classifier for our data (almost 98%), followed by SVM (almost 96%) and then ANN (almost 93%) [11].

While studies on fraud and ad blocking have been strengthened with machine learning methods, blockchain technology, which brings new approaches and measures to data privacy and security, has also been used in recent years. Researchers have started this process by examining the fraud systems that can be realized in blockchain transactions [12, 13]. Zou et al. proposed a model that integrates the idea of blockchain into crowd sensing to avoid security issues such as rejection and stamping of information from the traditional centralized crowd sensing system. They conducted experiments on the average running time of block production related to their proposed blockchain structure. They analyzed the effect of different conditions on success rate, time, efficiency and robustness [14]. Liu and Lee proposed a blockchain-based model that can prevent mobile frauds that may occur in refunds through mobile applications [15]. Saldamli et al. implemented a blockchain-based system to prevent fraudulent activities in health insurance transactions. This study is based on record-keeping logic. In the light of their findings, they state that they provide a secure platform and that there is no significant delay in transaction processes [16]. Zhang et al. studied the same topic as Saldamli with different methods. Zhang et al. proposed a new detection and protection system by combining blockchain technology with deep learning methods. They concluded that the proposed approach can reduce the workload of health insurance auditors and increase efficiency. Experiments on two real datasets from 3 hospitals show that the solution can effectively realize anti-fraud medical insurance [17]. Figure 1 shows the bibliographic analysis of the blockchain and fraud keywords obtained in the

literature review.

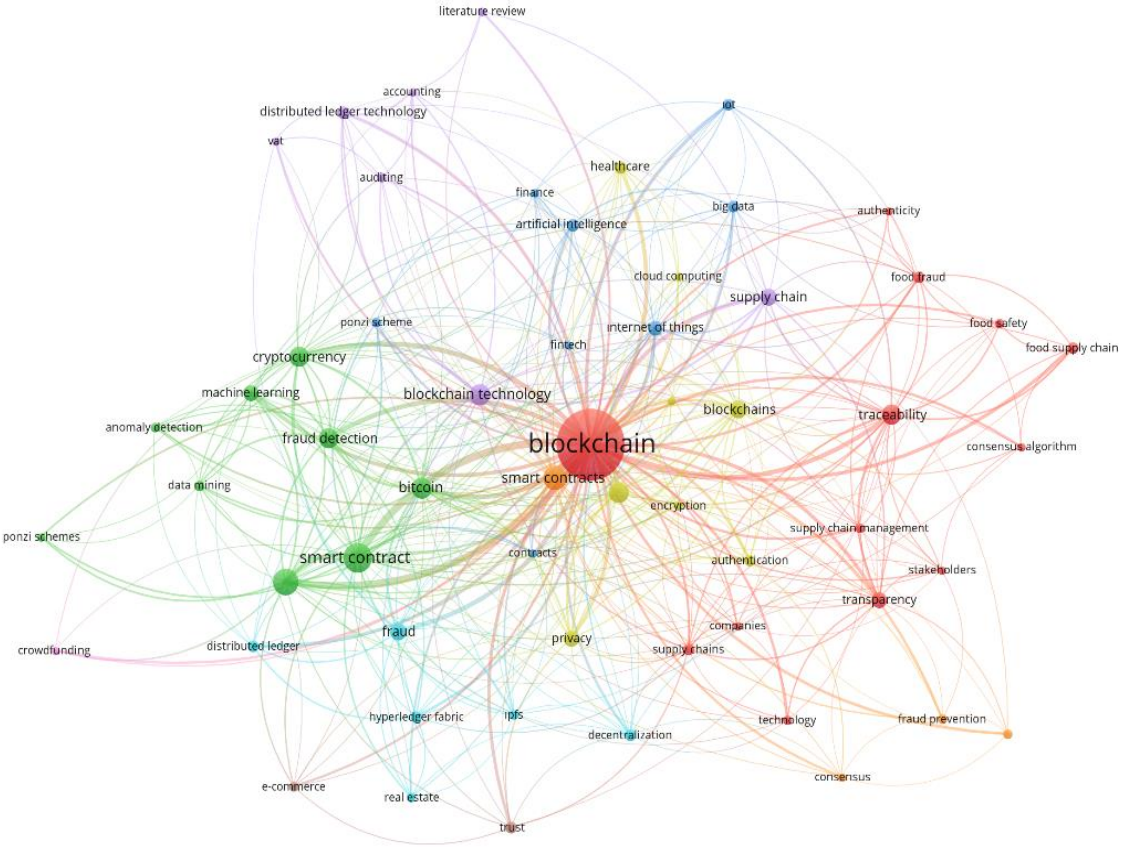


Fig.1. Keyword distribution of fraud and blockchain studies

On 30.04.2023, 500 results were reached in the research conducted by selecting the "Topics" title with the keyword "Blockchain" and "Fraud". According to the years, 291 articles, 190 papers, 2 book chapters, 2 book chapters, 2 letters, 15 early appearance studies were reached from different disciplines and fields, the oldest being 2015 and the newest being 2023. The data were analyzed by author-citation-journal-country-institution-keyword and abstract analysis. The contents indexed in Web of Science were taken as the database.

3. Proposed Model, Findings and Discussions

In this study, a blockchain structure based on the Proof of Work (PoW) algorithm is prepared and used. We chose this algorithm because its transparency and security methods are highly compatible with the proposed model. PoW (Proof of Work) is a consensus mechanism used to verify transactions on a blockchain network [18]. This mechanism is used in many blockchain networks such as Bitcoin and many other cryptocurrencies. The PoW structure is based on solving a mathematically challenging problem. This problem requires setting the header of a block to be less than or equal to a target value using hash functions. This target value is set based on the difficulty of the block, and users in the network know that this problem must be solved to prove the correctness and validity of the block. The PoW mechanism is resistant to double-spending attacks to ensure the security of the network. A double-spending attack is a type of attack where a person tries to spend the same currency more than once. However, the PoW structure prevents such attacks because for a block to be valid, it must be verified by previous blocks. In summary, the PoW consensus mechanism is based on a mathematical problem solving to secure the network and prove the correctness and validity of each block in the blockchain [19, 20].

Due to the anonymity of the application users' identities and the competition between users during the verification of transactions, PoW cannot be said to be completely transparent. However, competition between users increases the security of the network and ensures the authenticity of transactions. The transparency of PoW is enhanced by the fact that every transaction on the blockchain is public. Any person can inspect and verify any transaction on the blockchain. As a result, although the PoW consensus mechanism is not completely transparent due to competition between users, the level of transparency is quite high due to the public nature of the transactions in the blockchain [21]. Figure 2 illustrates the architecture showing the transaction processes and outcomes faced by phone numbers making calls for fraud, advertising, or survey purposes.

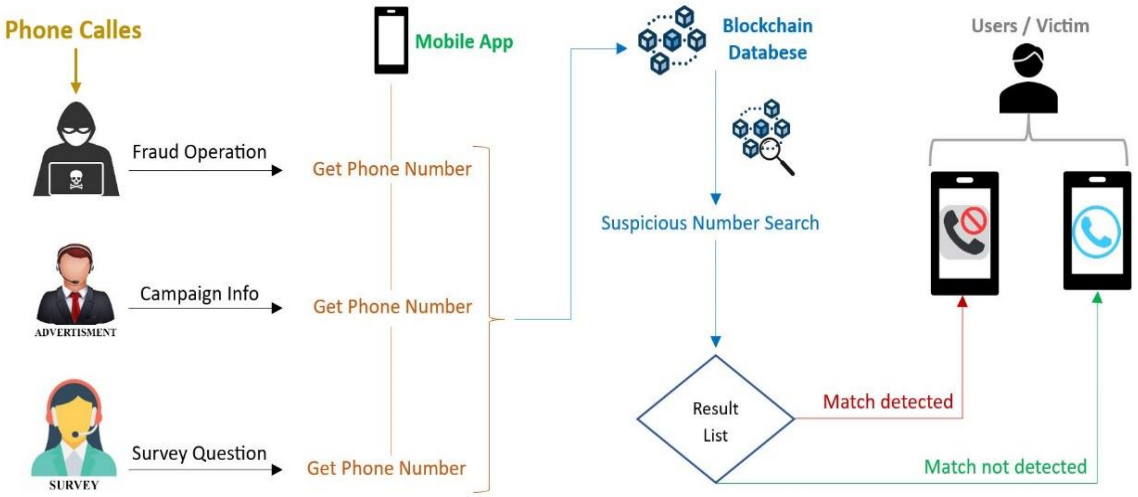


Fig.2. Blocking architecture for registered fraud and advertising calls

The calling number is received by the mobile application and queried from the blockchain-based database, where the calling numbers and whistleblowers were previously registered. As a result of the query, the app will either block the call and show a notification or allow the call. Figure 3 shows the process and verification method when the app users make a report.

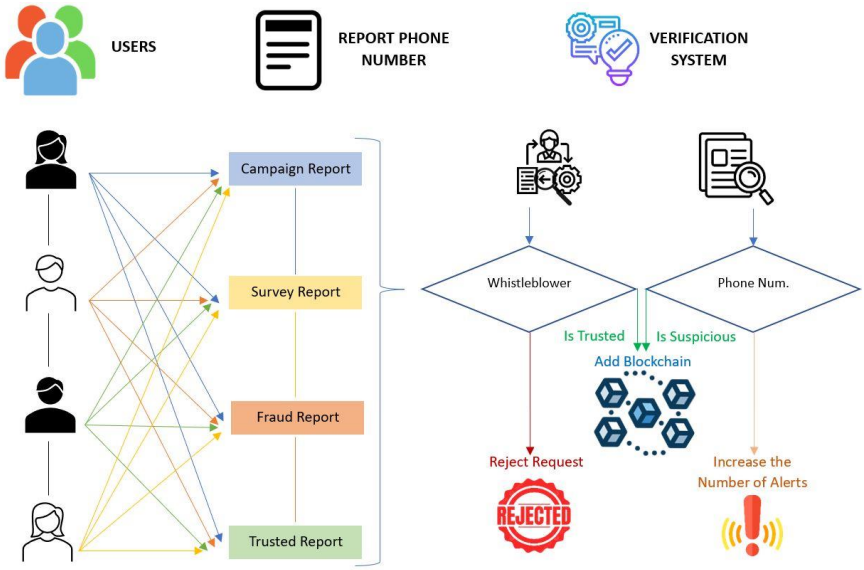


Fig.3. Blocking architecture for registered fraud and advertising calls

```
const SHA256 = require('crypto-js/sha256');
const express = require('express');
const http = require('http');
const WebSocket  = new require('ws');
//const wss = new ws.Server({noServer: true});
const clients = new Set();

const app = express();

let found = false;
let activeBlock;
let difficulty=1;
let chainLength=1;
let maxLength=1000;
let timerStart=false;
let strPrefix = Array(difficulty + 1).join("0");
```

Fig.4. Blockchain startup predefinitions and architecture configuration

The blockchain structure that the proposed application uses as a database is prepared in javascript language. Some of the method and class codes prepared during blockchain creation are shared in the study. Figure 4 shows the code for the constant definitions, protocols and initialization settings required for the blockchain structure.

In Figure 5, a blockchain class named Block is defined and a constructor method is prepared for this class. Within this class, a method called "calculateHash" is created to calculate the hash. This method is designed to combine the values of the new block data to be added to the chain using the SHA256 Hash algorithm and to calculate and return the eigenvalue of this combined value.

```
class Block{
    constructor (index, timestamp, data, previousHash = ''){
        this.index = index;
        this.timestamp = timestamp;
        this.data = data;
        this.previousHash = previousHash;
        this.nonce = 0;
    }
    calculateHash(){
        return SHA256(this.index + this.previousHash +
        this.timestamp + JSON.stringify(this.data) + this.nonce).toString();
    }
}
```

Fig.5. Block class and methods

Figure 6 shows the Blockchain class and the methods written in it. There is a constructor method in the Blockchain class. In this constructor method, the Genesis block, which is the starting block for the blockchain, is created. In addition, the difficulty level of the blockchain is set. Just below the constructor method is a method called "createGenesisBlock" which creates the Genesis block. The method called "getLatestBlok" reads the last block added to the blockchain, which is used when adding data to the blockchain. "addBlock", which works in asynchronous mode, is the method that adds a new block to the blockchain. The validity of the chain is ensured by the method "isChainValid".

```
class Blockchain{
    constructor(){
        this.chain = [this.createGenesisBlock()];
        this.difficulty = 1;
    }
    createGenesisBlock(){
        return new Block(0, "23/04/2023", "Genesis Block", "0");
    }
    getlatestBlock(){
        return this.chain[this.chain.length - 1];
    }
    async addBlock(newBlock){
        newBlock.previousHash = this.getlatestBlock().hash;
        while(found!==true){
            ;
        }
        found=false;
    }
    isChainValid(){
        for(let i = 1; i < this.chain.length; i++){
            const currentBlock = this.chain[i];
            const previousBlock = this.chain[i-1];

            if(currentBlock.hash !== currentBlock.calculateHash()){
                return false;
            }

            if(currentBlock.previousHash !== previousBlock.hash){
                return false;
            }
        }
        return true;
    }
}
```

Fig.6. Blockchain class and methods

4. Findings and Discussions

In order to determine the most effective and optimum working performances of the prepared blockchain structure, various tests were performed. The results obtained from these performance tests are shown in Table 1. The blockchain

structure was run at 5 different difficulty levels and 10 different metric values were obtained. In these values, the number of records was kept constant, and the difficulty levels were changed. Different metric values, including average time, median, minimum, and maximum time, were obtained in meticulous measurements.

Table 1. Metric values measured by blockchain difficulty level

Metrics/Time (ms)	Difficulty 1	Difficulty 2	Difficulty 3	Difficulty 4	Difficulty 5
Mean	0,35	2,60	28,02	490,55	7.179,13
Standard Error	0,04	0,26	2,47	49,04	651,60
Median	0,25	1,82	21,12	338,39	6.339,00
Mode	0,13	0,35	#N/A	#N/A	#N/A
Standard Deviation	0,36	2,62	24,71	490,36	6.516,00
Sample Variance	0,13	6,86	610,75	240.448,68	42.458.236,57
Kurtosis	20,18	8,29	2,35	2,70	1,57
Skewness	3,98	2,41	1,56	1,69	1,29
Range	2,56	16,13	118,69	2.366,48	29.055,15
Minimum	0,08	0,13	0,19	1,52	14,85
Maximum	2,64	16,26	118,87	2368,00	29070,00
Sum	34,66	260,25	2.802,13	49.054,78	717.913,28
Count	100,00	100,00	100,00	100,00	100,00

Two different statistical tests are used to determine whether a given group of scores is drawn from a normal or bell curve distribution. These are the skewness and kurtosis tests. Skewness measures the degree to which a distribution is not symmetric [22], while kurtosis is an index of the degree to which there are too many or too few samples in the middle of the distribution [23]. Most of the scores obtained are to the left of the mean. Therefore, values smaller than the mean make this distribution positively skewed. As can be seen from Table 1, as the difficulty level increases, the realization time of the recordings increases. This increase is shown graphically in Figure 6. The reason for the increase in data recording times as the difficulty level increases can be seen in the details of Figure 7. In Figure 7, the increase in the mining time of users to add records according to the difficulty level increases the processing time of the whole process.

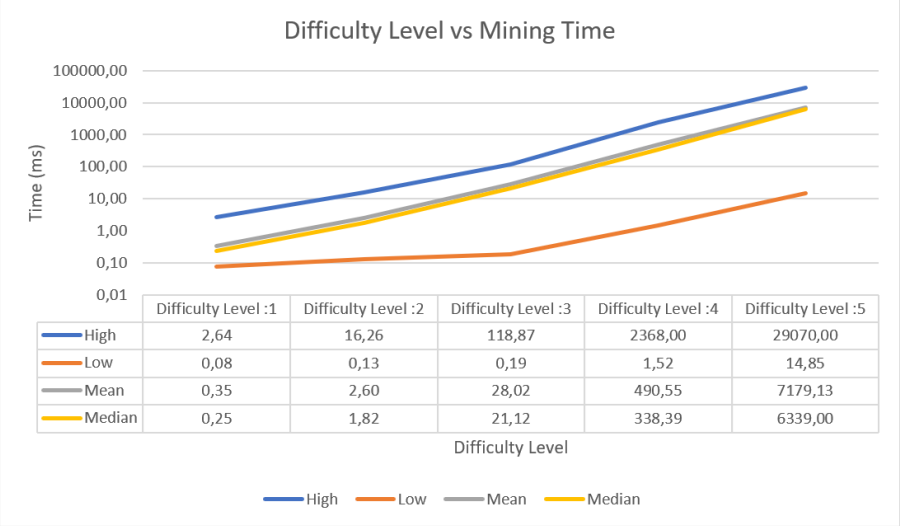


Fig.7. Measurement of mining time by blockchain difficulty level

Figure 8 shows the graph of average and total times by performing operations with different number of records at the first level difficulty. At the first level of difficulty, performance was measured with data numbers ranging from 1000 to 10,000,000. In the obtained graph, it is observed that the total time increases linearly, while the average time remains at approximately the same value after 10,000 records. The reason why the average time graph is high at the beginning and decreases and stabilizes as the number of records increases is due to the addition time of the genesis block created in the blockchain structure at the beginning. As the number of records increases, the time to create a genesis block within the time value does not affect the value in the graph as it approaches the average transaction execution time. In the light of this data, it is seen that the first level difficulty value performs quite well in a multi-user system.

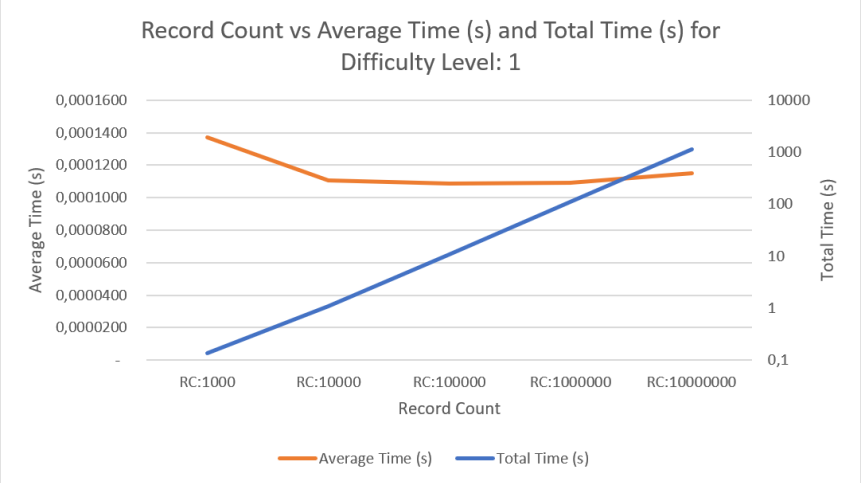


Fig.8. Data processing times by number of records at blockchain difficulty level one

The mobile application we propose in this study has a blockchain-based storage system and carries out processes that record and take precautions against real users' calls. The developed application was used by 72 people for 42 days and the users' evaluations of the application are shown in Figure 9.

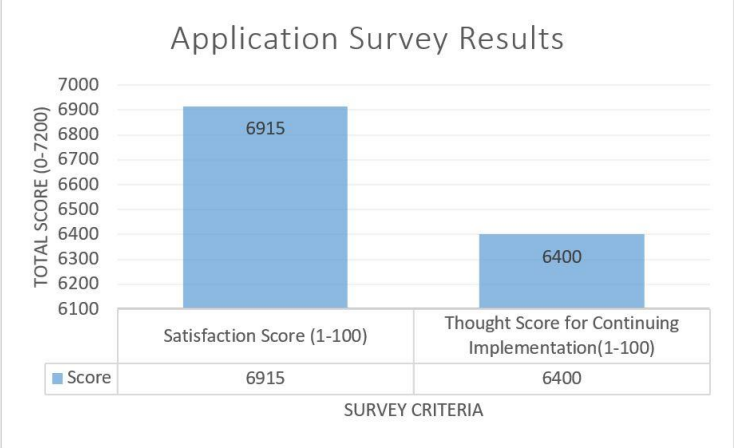


Fig.9. Application survey result

When the users rated their satisfaction with the application between 0 and 100 points, the application received 6915 points out of 7200, with an average score of 96 points. This result shows us that the application was found successful by the users. In addition to this, users gave a total of 6400 points to the question of whether they will continue to use the application, with an average of approximately 88% in favour of continuing.

5. Conclusions

Mobile phone calls are the most preferred electronic communication methods in daily life. These calls can be made for business purposes as well as for natural reasons. Users may not want to be disturbed by mobile phones during busy work or rest hours, even at normal times. At this stage, it is very important to identify normal user calls and calls for fraud, advertising, campaigns or surveys. In this study, a blockchain-based model for blocking fraud and harassment notifications is proposed. In the results obtained after the tests of the model, metric values reveal the success of the model. In addition, the optimum values of the difficulty levels as a result of the performance measurements of the blockchain system were determined. Considering the delay times in performance measurements, the security quality provided makes the delay acceptable. The satisfaction and usefulness ratings given by the application users also have a positive impression that the system can be implemented. This result is a positive evaluation in terms of the continuity of the application. In future studies, it is aimed to improve the application by adding smart contracts to the application base, to include messages as well as calls in the system and to prepare new versions.

References

[1] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Discovery of ranking fraud for mobile apps," IEEE Trans Knowl Data Eng, vol. 27, no. 1, pp. 74–87, Jan. 2015, doi: 10.1109/TKDE.2014.2320733.

[2] M. Yelland, "Fraud in mobile networks," Computer Fraud & Security, vol. 2013, no. 3, pp. 5–9, Mar. 2013, doi: 10.1016/S1361-3723(13)70027-7.

[3] "Canada News Today | CTV News." https://www.ctvnews.ca/canada/saad-salman-1.5260052 (accessed Apr. 28, 2023).

[4] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[5] A. Kamišalić, R. Kramberger, and I. Fister, "Synergy of Blockchain Technology and Data Mining Techniques for Anomaly Detection," Applied Sciences 2021, Vol. 11, Page 7987, vol. 11, no. 17, p. 7987, Aug. 2021, doi: 10.3390/APP11177987.

[6] X. Zhang, R. Qin, Y. Yuan, and F. Y. Wang, "An Analysis of Blockchain-based Bitcoin Mining Difficulty: Techniques and Principles," Proceedings 2018 Chinese Automation Congress, CAC 2018, pp. 1184–1189, Jan. 2019, doi: 10.1109/CAC.2018.8623140.

[7] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer Peer Netw Appl, vol. 9, no. 2, pp. 397–413, Mar. 2016, doi: 10.1007/S12083-015-0347-X/TABLES/3.

[8] Y. Lin et al., "Dynamic Control of Fraud Information Spreading in Mobile Social Networks," IEEE Trans Syst Man Cybern Syst, vol. 51, no. 6, pp. 3725–3738, Jun. 2021, doi: 10.1109/TSMC.2019.2930908.

[9] C. M. R. Haider, A. Iqbal, A. H. Rahman, and M. S. Rahman, "An ensemble learning based approach for impression fraud detection in mobile advertising," Journal of Network and Computer Applications, vol. 112, pp. 126–141, Jun. 2018, doi: 10.1016/J.JNCA.2018.02.021.

[10] H. Grosser, P. Britos, and R. García-Martínez, "Detecting fraud in mobile telephony using neural networks," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 3533 LNAI, pp. 613–615, 2005, doi: 10.1007/11504894_85/COVER.

[11] R. Mouawi, M. Awad, A. Chehab, I. H. El Hajj, and A. Kayssi, "Towards a Machine Learning Approach for Detecting Click Fraud in Mobile Advertizing," Proceedings of the 2018 13th International Conference on Innovations in Information Technology, IIT 2018, pp. 88–92, Jan. 2019, doi: 10.1109/INNOVATIONS.2018.8605973.

[12] P. O. Goffard, "Fraud risk assessment within blockchain transactions," Adv Appl Probab, vol. 51, no. 2, pp. 443–467, Jun. 2019, doi: 10.1017/APR.2019.18.

[13] P. Joshi, S. Kumar, D. Kumar, and A. K. Singh, "A Blockchain Based Framework for Fraud Detection," 2nd International Conference on Next Generation Computing Applications 2019, NextComp 2019 - Proceedings, Sep. 2019, doi: 10.1109/NEXTCOMP.2019.8883647.

[14] S. Zou, J. Xi, H. Wang, and G. Xu, "CrowdBLPS: A Blockchain-Based Location-Privacy-Preserving Mobile Crowdsensing System," IEEE Trans Industr Inform, vol. 16, no. 6, pp. 4206–4218, Jun. 2020, doi: 10.1109/TII.2019.2957791.

[15] D. Liu and J. H. Lee, "CFLedger: Preventing chargeback fraud with blockchain," ICT Express, vol. 8, no. 3, pp. 352–356, Sep. 2022, doi: 10.1016/J.ICTE.2021.06.001.

[16] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh, "Health Care Insurance Fraud Detection Using Blockchain," 2020 7th International Conference on Software Defined Systems, SDS 2020, pp. 145–152, Apr. 2020, doi: 10.1109/SDS49854.2020.9143900.

[17] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. P. C. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," Future Generation Computer Systems, vol. 130, pp. 140–154, May 2022, doi: 10.1016/J.FUTURE.2021.12.006.

[18] M. Kara et al., "A Compute and Wait in PoW (CW-PoW) Consensus Algorithm for Preserving Energy Consumption," Applied Sciences 2021, Vol. 11, Page 6750, vol. 11, no. 15, p. 6750, Jul. 2021, doi: 10.3390/APP11156750.

[19] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," Proceedings of the ACM Conference on Computer and Communications Security, vol. 24-28-October-2016, pp. 3–16, Oct. 2016, doi: 10.1145/2976749.2978341.

[20] W. Ren, J. Hu, T. Zhu, Y. Ren, and K. K. R. Choo, "A flexible method to defend against computationally resourceful miners in blockchain proof of work," Inf Sci (N Y), vol. 507, pp. 161–171, Jan. 2020, doi: 10.1016/J.INS.2019.08.031.

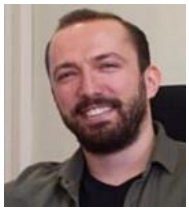
[21] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "On Blockchain Integration with Supply Chain: Overview on Data Transparency," Logistics 2021, Vol. 5, Page 46, vol. 5, no. 3, p. 46, Jul. 2021, doi: 10.3390/LOGISTICS5030046.

[22] R. A. Groeneveld and G. Meeden, "Measuring Skewness and Kurtosis," Journal of the Royal Statistical Society: Series D (The Statistician), vol. 33, no. 4, pp. 391–399, Dec. 1984, doi: 10.2307/2987742.

[23] D. N. Joanes and C. A. Gill, "Comparing measures of sample skewness and kurtosis," Journal of the Royal Statistical Society: Series D (The Statistician), vol. 47, no. 1, pp. 183–189, Apr. 1998, doi: 10.1111/1467-9884.00122.

Authors' Profiles

Remzi GÜRFİDAN is working as a Ph.D. of cyber security application and researching center at Isparta University of Applied Sciences. He completed his master's degree in electronic and computer department. He has program development experience cyber security, deep learning, and software development. He has 2 books in the field of blockchain technologies. He has been editor-in-chief of the journal in two international journals in the field of engineering.



Şerafettin ATMACA is working software application and researching center at Isparta University of Applied Sciences. He completed his master's degree in the computer engineering department. He has program development experience deep learning, and software development.

How to cite this paper: Remzi Gürfidan, Şerafettin Atmaca, "Blocking Fraud, Advertising, or Campaign-Related Calls with a Blockchain-based Mobile App", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.5, pp.14-22, 2024. DOI:10.5815/ijcnis.2024.05.02