MBNA Publishing House Constanta 2021

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Blockchain Technology for Maritime Industry

To cite this article: Stefania Loredana NITA, Marius Iulian MIHAILESCU and Ciprian RACUCIU, Proceedings of the International Scientific Conference SEA-CONF 2021, pg.219-223.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-21-029

Blockchain Technology for Maritime Industry

Stefania Loredana Nita[1], Marius Iulian Mihailescu[2], Ciprian Racuciu[3]

[1]Institute for Computers, Integrated Systems Department, Bucharest, Romania
[2]Spiru Haret University, Scientific Research Center in Mathematics and Computer Science, Bucharest, Romania
[3]Titu Maiorescu University, Computer Science Department, Bucharest, Romania

E-mail: stefania.nita@outlook.com

Abstract. Blockchain technology has gained its place among the most important technologies nowadays. The unique characteristic of the blockchain is that it is implemented as a distributed ledger comparing with the traditional database management systems, therefore it is independent of a central authority. Moreover, blockchain contains cryptographic mechanisms that protect the data and ensures integrity. In this paper, we present the advantages of using blockchain in the maritime industry and propose a blockchain-based framework for this field.

1. Introduction

Blockchain Technology, also called Distributed Ledger Technology (DLT), provides a secure approach for transactions that eliminates the need for a central authority. It was introduced in 2008 by a group under the pseudonym Satoshi Nakamoto, who implemented the Bitcoin and released its white paper [1]. Blockchain has gained its place among the most important technologies nowadays because it can be used for reducing risks, avoiding fraud, and bringing transparency. Moreover, it is scalable and can be applied in many activity domains.

The main elements of a blockchain structure are block, node, and miner [2]. A *block* usually is made of three components, namely the data itself, a random nonce based on which the header hash of the block is generated, and the hash seeded by the nonce. More blocks form a chain and each block contains its own nonce and hash, which are unique, and additionally a referring to the preceding block's hash. A *node* is represented by any device that has copies of the chain and helps the network to be functional. Note that a blockchain network is decentralized, functioning on a peer-to-peer basis, therefore each node communicates with all other nodes and has its own copy of the blockchain. The network should be programmed to apply specific algorithms to update, trust and examine new blocks. Lastly, a *miner* creates a block. To create a block, the miner must resolve a very difficult math problem that finds a nonce that produces an acknowledged hash. When such nonce is discovered, the block is added to the chain. To perform a transaction, the network can be programmed to use one of the following techniques to allow nodes to validate the transaction: *Proof-of-Work* (PoW) and *Proof-of-Stake* (PoS). The first algorithm is used to prove that the nodes have enough computational power to make transactions, while the other technique is used to make sure that the nodes have enough coins to validate the transactions.

From the above description, we can conclude the following characteristics of a blockchain network: *decentralization* (there is no central authority), *persistency* (each node has a copy of the blockchain), *anonymity* (users that launch interactions with the network have generated addresses), and *audibility* (each transaction is validated before being added to the blockchain and it can be easily reviewed).

Blockchain can be applied in many activity domains, such as finance [3], [4], education [5], healthcare [6], logistics [7], manufacturing [8], [9], energy [10], robotics [11], [12], etc. In 2020 the global blockchain market worthen USD 3.0 billion and it is predicted to grow to USD 39.7 billion by 2025 [13].

The paper is organized as follows: in the current section, we presented general information about blockchain, in the second section, we present the solutions for the maritime industry based on blockchain technology. In addition, we present the advantages and the disadvantages of this approach. In the third section, we describe our proposed framework that uses blockchain technology applied in the maritime industry and discuss its security and practical results. Finally, we present the conclusions of the paper.

2. Blockchain for the Maritime Industry

In this section, we present important results achieved in using blockchain for the maritime industry.

In the work [14], the authors propose a system that manages the digital identities of the participants in the blockchain network. When a potential participant adheres to the network, a pair of public and private keys are generated for this user and a digital certificate (based on the public key and digital signatures) that will represent its digital identity and will be later used by the user to be recognized by the blockchain participants. After it is accepted in the network, the participant uses its private key to sign operations and the rest of the participants check the validity of the transaction by checking the digital signatures. Further, the authors provide a use case for their management system, regarding the moment when the cargo is changed between two participants.

In [15] the authors have another approach of using blockchain in maritime. Here, the private blockchain is used in the authentication process for the IoT (Internet of Things) devices from the ships. The authors prove their solution can be used for intrusion avoidance and analyze the impact of this implementation on the overall performance of the system, showing that it is sustainable and effective.

As stated in [16] blockchain can have an economic impact on maritime transport. Here, the authors make a study about the use of blockchain for information exchanging and show how it can influence sustainability from an environmental and social point of view.

In [17] the authors propose a blockchain-based system for real-time ship tracking, in which the smart contracts are replacing the physical documents. Also, they show that using blockchain it can lead to a less centralized logistics field worldwide.

Blockchain technology can be roughly seen as a distributed database that can be consulted at any time, providing data whose integrity is preserved. For the maritime industry, blockchain has many advantages from which we can mention:

- *Privacy*: the network works on a peer-to-peer basis, while the interactions between them are secured using cryptographic mechanisms. Moreover, users are assigned an encrypted unique identifier, which makes their identities protected and each node in the network may safeguard sensitive data, for example, information about customers. These aspects can be translated into the maritime industry in the fact that all entities involved in the shipment process can access data anytime and can generate a trail of secure audits for the shipments.
- *Integrity and security*: the encryption of one record is separate from all other records, and the keys used are related to the nodes that participated in the transaction. Additionally, the record is registered by each node in the network. Due to its functioning mechanism, blockchain does not allow altering a record once it was registered. This is useful in the maritime industry because, on one hand, all operations are encrypted and registered properly, and on the other hand, they cannot be denied and are available for all participants involved.
- *Confidence*: the accuracy in blockchain reaches a high degree, because as it was seen it cannot be altered once registered and the ledger can be seen by all participants simultaneously and in real-time. With this characteristic, the advantage in the maritime industry is that the logistic process can be managed better.
- *Availability and reduced costs*: it can be clearly seen that the information is available at any moment. Are implemented in the smart contracts, representing pieces of code that are executed

any time when a transaction needs to be validated, ensuring that the rules of the blockchain network are followed. The costs are reduced from different points of view, for example, the physical paper is eliminated from the process, administrative mistakes are avoided and the operations become more efficient, as they become digital.

3. The proposed framework

In this section, we present the proposed framework that is designed for maritime environments that work with documents. Our framework includes a searchable encryption scheme, whose search operation is based on blockchain technology. Searchable encryption (SE) is a cryptographic mechanism that allows the data user to search over encrypted data. In general, there are four entities involved in a searchable encryption system, namely, trusted authority (TA), data owner (DO), data user (DU), cloud server (S). Every entity has its specific characteristics as follows: TA generates the system parameter and generates the pair containing the public and the private key for DO, DU and S, DO owns the data, encrypts it and send it to the server, DU generates search queries and decrypts the results, S performs the search query over encrypted data and sends the results to DO. The workflow for searchable encryption is presented in Figure 1.

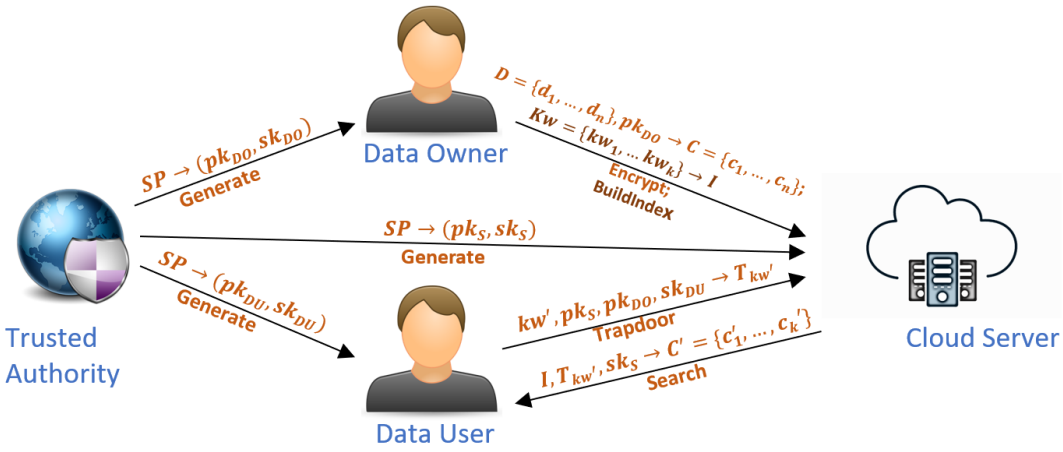

Figure 1. The general workflow in a general SE scheme

The algorithms included in our framework are:

- $Setup(\lambda) \rightarrow SP$. Based on the security parameter λ, TA generates the parameters of the system.
- $Generate(SP) \rightarrow ((pk_S, sk_S), (pk_{DO}, sk_{DO}), (pk_{DU}, sk_{DU}))$. Using the security parameters SP generated above, TA generates the keys in the form $(publicKey, secretKey)$ for the other entities.
- $Encrypt(D, pk_{DO}) \rightarrow C$. Using its public key pk_{DO}, DO encrypts the set of the owned documents $D = \{d_1, \dots, d_n\}$, resulting the encryption $C = \{c_1, \dots c_n\}$ of these documents. Then DO sends the encrypted documents to S.
- $BuildIndex(Kw, pk_{DU}) \rightarrow I$. DO performs the algorithm for building the index structure using DU's public key pk_{DU} and set of keywords $Kw = \{kw_1, \dots, kw_k\}$ that characterize the documents. In this step intervenes the modification of the traditional SE scheme, because DO sends the index structure (which is encrypted) to the blockchain network (BN).
- $Trapdoor(kw', pk_S, pk_{DO}, sk_{DU}) \rightarrow T_{2kw'}$. DU uses for running this algorithm more parameters: the keyword kw' that needs to be searched, DO's public key $pk_{DO}$and his/her own private key sk_{DU} based on which it is generated a link-value $T_{1kw'}$. Then the server performs a checking algorithm using the link-value $T_{1kw'}$ and its private key sk_S, resulting the final trapdoor value $T_{2kw'}$, which S sends to BN.

- $Search(I, T_{2kw'}) \rightarrow C'$. The blockchain network performs the search process, as follows: firstly, it checks that the timestamp of the transaction for the search query is less than the standard one, which is contained in the smart contract of BN. If so, then proceed further, otherwise, reject the transaction. Then, BN checks whether the node of the user that submitted the search query has enough computational power. If so, then passes to the next step, otherwise rejects the transaction. The final step is the search process. Using the index structure I and the trapdoor $T_{2kw'}$, BN returns the encrypted indexes that match the search criteria, i.e. $T_{2kw'}$, sends them to S and then validates the transaction. On its side, S transmits to DU the encrypted documents C' corresponding to encrypted indexes.
- $Decrypt(C', sk_{DU}) \rightarrow D'$. After receiving the encrypted documents C', DU decrypts them using the secret key and obtains the set of plain documents D'.

The correctness of the proposed framework consists in the fact that for any trapdoor generated based on a valid keyword, then the search algorithm returns the correct corresponding encrypted documents, namely

$$P[Search(I, T_{2kw'}) \neq \emptyset : T_{2kw'} = Trapdoor(kw', pk_S, pk_{DO}, sk_{DU})] = 1,$$

where the symbol $\emptyset$ represents the empty set.

Our proposed framework has the following security characteristics:

Integrity. Since the search process is made on the blockchain network, this ensures the integrity of the process.

Non-repudiation. When a search transaction is completed, it is registered by any node in the network, therefore, it is extremely difficult to deny a search operation.

Reliability. The search process is transparent and involves the participation of the server. A remark is the fact that in the system, the participants may use different encryption techniques for the indexes and for the documents, leading to a better security.

Fairness. Once the rules are established, these are registered in the smart contract of the blockchain and cannot be modified.

4. Conclusion

In this paper, we discussed the advantages of blockchain technology for the maritime domain and we have seen where it can be included to form secure and transparent systems. Another result of the paper is the searchable encryption framework that integrates the blockchain technology for encrypted document search in the cloud.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. – URL: https://bitcoin.org/bitcoin.pdf.

[2] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[3] Hileman, G., & Rauchs, M. (2017). Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance, 33, 33-113.

[4] Cohn, A., West, T., & Parker, C. (2017). Smart after all: blockchain, smart contracts, parametric insurance, and smart energy grids. Georgetown law technology review, 1(2), 273-304.

[5] Albeanu, G. (2017, October). Blockchain technology and education. In The 12th International Conference on Virtual Learning ICVL (pp. 271-275).

[6] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 1-8.

[7] Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat?. In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23 (pp. 3-18). Berlin: epubli GmbH.

[8] Kennedy, Z. C., Stephenson, D. E., Christ, J. F., Pope, T. R., Arey, B. W., Barrett, C. A., & Warner, M. G. (2017). Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. Journal of Materials Chemistry C, 5(37), 9570-9578.
[9] Barenji, A. V., Li, Z., & Wang, W. M. (2018, June). Blockchain cloud manufacturing: Shop floor and machine level. In Smart SysTech 2018; European Conference on Smart Objects, Systems and Technologies (pp. 1-6). VDE.
[10] Münsing, E., Mather, J., & Moura, S. (2017, August). Blockchains for decentralized optimization of energy resources in microgrid networks. In 2017 IEEE conference on control technology and applications (CCTA) (pp. 2164-2171). IEEE.
[11] Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M. (2018). Blockchain based decentralized management of demand response programs in smart energy grids. Sensors, 18(1), 162.
[12] Ferrer, E. C. (2018, November). The blockchain: a new framework for robotic swarm systems. In Proceedings of the future technologies conference (pp. 1037-1058). Springer, Cham.
[13] De Meijer, C.R.W (2020, December). Blockchain trends in 2021: Expect the unexpected. URL: https://www.finextra.com/blogposting/19679/blockchain-trends-in-2021-expect-the-unexpected
[14] Xu, L., Chen, L., Gao, Z., Chang, Y., Iakovou, E., & Shi, W. (2018, October). Binding the physical and cyber worlds: A blockchain approach for cargo supply chain security enhancement. In *2018 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-5). IEEE.
[15] Rahimi, P., Khan, N. D., Chrysostomou, C., Vassiliou, V., & Nazir, B. (2020, May). A Secure Communication for Maritime IoT Applications Using Blockchain Technology. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 244-251). IEEE.
[16] Jović, M., Tijan, E., Žgaljić, D., & Aksentijević, S. (2020). Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange. *Sustainability, 12*(21), 8866.
[17] Grzelakowski, A. S. (2019). Global container shipping market development and Its impact on mega logistics system. *TransNav: International Journal on Maritime Navigation and Safety of Sea Transportation, 13*.