Original Scientific Paper

Journal of Applied Engineering Science

doi:10.5937/jaes17-22740

Paper number: 17(2019)3, 613, 333 - 337

# BLOCKCHAIN SECURITY OF AUTONOMOUS MARITIME TRANSPORT

*Miro Petković[1]*, Vice Mihanović[2], Igor Vujović[1]*

*[1]University of Split, Faculty of Maritime studies, Croatia*

*[2]Split Port Authority, Croatia*

*Autonomous ships are in experimental stage nowadays with Maritime Autonomous Surface Ships (MASS) already defined by IMO. Since MASS rely heavily on communications, security of communication systems and data security is critical. Secure communication is required to avoid bad actors to interfere with the communications or seizing control of a autonomous ship. In this paper, implementation of blockchain technology to improve autonomous vessels control security is investigated. This technology is already used in maritime bill of lading, acts on ship's technical inspection and for more accurate container tracking etc. The paper is organized as follows: first section describes current status on autonomous ships, basic definitions and terms, second section describes what is blockchain technology and how does it work, third section deals with blockchain technology applications with the proposed usage of the technology in autonomous vessels control scheme.*

*Key words: MASS, blockchain technology, security, communications*

## INTRODUCTION

Marine Autonomous Surface Ships (MASS) are becoming reality. First autonomous ferries are under testing since 2018 in Finland [1] and small autonomous Unmanned Surface Vessels (USV's) are widely used in ocean research, coast guard and military applications etc. Remotely operated local vessels are expected by 2020 and ocean-going ships for maritime transport by 2030 [2].

In this paper, improving security of communication systems and data security of MASS ships using new technologies is investigated. Since connectivity is a critical component of MASS, communication need to be two-way, secure and supported by multiple systems. Secure communication is mandatory, to avoid bad actors to interfere with ships communication or taking the control of the ship [3].

Security based on blockchain technology (BT) is proposed to enable secure communication and secure data storage exchanged between MASS and shore control center. Implementation of BT will eliminate some threats for ships communication, i.e. losing the data, data change by bad actors or data hijacking [2]. BT will play a major role in identification and certification, ensuring data integrity and information security.

## AUTONOMOUS SHIPS CURRENT STATUS

Automated ships can be divided into two groups: MASS and unmanned surface vehicle (USV). Moreover, if we differentiate MASS by control level and legal regulation, we can group them into four classes [4]: Autonomy Assisted Bridge (AAB), Periodically Unmanned Bridge (PUB), Periodically Unmanned Ship (PUS) and Continuously Unmanned Ships (CUS). Benefit of autonomous ships is elimination of human errors as a cause of accidents [5], and to obtain faster, safer, more precise, productive and cheaper ship's operation. Research done by [6] on MUNIN project in 2018 pointed out three topics for future design of autonomous ships:

- New hull design ( no crew onboard means no need for habitat, toilet, resting, etc. )
- Introduction of new fuel types ( LNG as a thrust fuel)
- Alternative modes of operation (more ships in convoys)

MASS require programming of voyage path, navigation and collision avoidance systems. International collision avoidance rules (COLREG) should be taken into consideration. Also, situation awareness protocols should be included e.g. when visibility is low, standard procedure is to reduce speed. Ship's systems should be monitored by Shore Control Center (SCC) at all-time. SCC can be connected to MASS by any communication technology (GSM, VHF, WiMax or satellite) to send refreshed data relevant to ship's voyage.

Autonomous Ship Controller (ASC) consists of Autonomous Navigation System (ANS) and Autonomous Engine and Monitoring Control (AEMC). These systems should make independent navigation decisions while being monitored by SCC operator. Operator should identify all unexpected threats and errors and pass it to others involved in SCC operation. Human-Machine interface (HMI) could be taken into consideration as a new operator-ship interface. This interface could improve operator's knowledge and situation awareness with final goal of easier decision making.

Autonomous ships navigation can be divided into two groups: ship's with primary navigation and secondary navigation. Hybrid system can be combination of two general alternatives:

*mpetkovic@pfst.hr

- Remotely controlled ships, controlled by SCC operator through satellite link
- Self-guided automated ships with integrated advanced systems of decision making

### *BLOCKCHAIN CURRENT STATUS*

Blockchain is not a single technology or new one, it is a product of many existing technologies integrated into one. It is a reliable and unique database, decentralized and trustful. BT comprises of many peer-to-peer computers connected into self-organizing distributed network. This approach is completely different from the traditional distributed database, where data consistency is not guaranteed and communication between nodes can be non-existent or unreliable. Fundamental difference between BT and traditional distributed database is its ability to deal with conflicts, as described in [7].

Since BT is decentralized and distributed digital ledger, it can be used to record transaction across a network of peer-to-peer computers. Transactions, which are not necessarily finance or money related, are stored on immutable ledger and cannot be changed retroactively without changing all subsequent blocks and the collusion of the network [7] (to validate false block as correct one, 50% of the nodes are needed). Therefore, BT successfully withstood cyber-attacks for more than 10 years.

Fig. 1 shows simplified structure of blocks in Blockchain. Block is a data element connected through index information to form a chain like structure. Block structure contains the block header and block data, block header links the current block with previous block to ensure the integrity and consistency of the entire blockchain database [8]. When the new block is created and linked to the end of the chain, data index of the previous block forms the head of the new block, data information forms the block data, then the timestamp is attached [9]. Thus, blockchain data structure consist: a block (contains complete history) chain (proof off authentication) equals a timestamp, which is most important innovation in the blockchain technology.

The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work [7]. Most importantly, timestamps shows that the blocks are connected in chronological order and marks the time of each transaction on the blockchain, proving when and what has happened on the network.

Unlike centralized data architectures, BT does not record and store data on centralized data center. Instead, all nodes on the network work together to maintain all data. Their task is to act as validators because honest nodes are not going to accept an invalid transaction or block containing them. As described in [7], nodes are maintaining the data information of its own and other nodes, for verification. Hence, updating of block data relies on the fact that most nodes or all of them consider data correct and authenticity is approved. Hacking or damaging one of the nodes will not affect the data.

There are several approaches to BT architecture, they are categorized as Private, Permissioned or Public. Main distinction between these architectures is within way the nodes are involved in securing and/or verifying the blockchain database and its entries. Difference in implementation has implications for some of the benefits of BT as represented in the Table 1.

### *BLOCKCHAIN IN MARITIME INDUSTRY*

Both MASS and BT are in top ten technologies that will change maritime industry [10]. Some work regarding implementation of BT into maritime industry has been done by [11] , they established consortium with a goal of building global shipping on blockchain that will improve data sharing. Result is in a pilot project of administrative and financial integration within international distribution chains . The shipping company Maersk invested in BT [12], they expect that “The shipping industry will save billions of dollars through more accurate container tracking capability and automating shipping transactions”.

In August 2018 container, processed with new blockchain based bill of lading, has been released successfully in Port of Koper, Slovenia [13]. The bill of lading for this shipment has been issued electronically and transferred with the secure and reliable public blockchain network in just few minutes instead of days or weeks. Chances

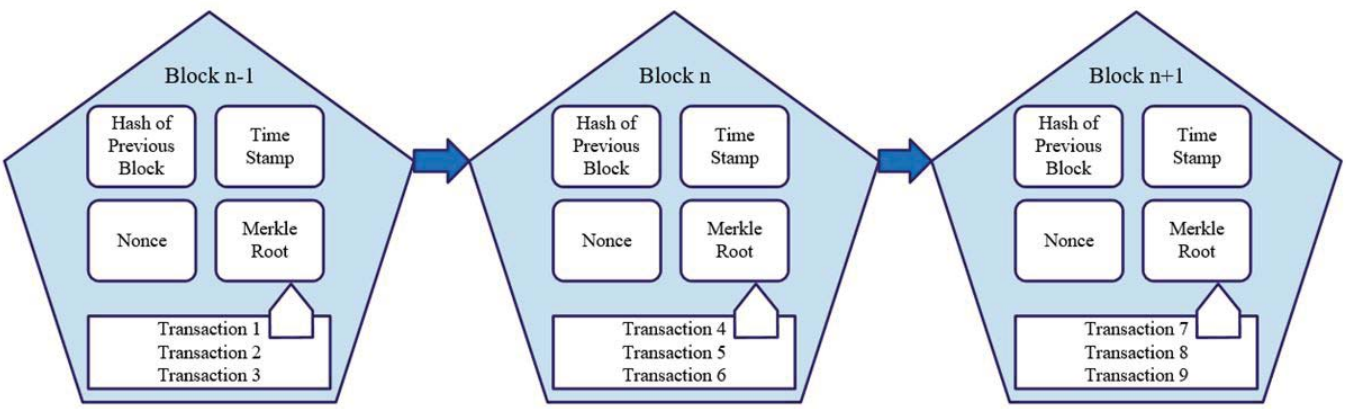


*Figure 1: Simplified structure of blocks*
*Source: Authors*

Table 1: BT architecture variance implementation benefits

| Architecture | Description | Decentralization | Immutability | Transparency |
|---|---|---|---|---|
| Private | Nodes are majorly or entirely run by a private party | None | None | Not Guaranteed |
| Permissioned (hybrid) | Nodes are run by 3rd parties who are granted specific permission by a private party | Low | Moderate | Not Guaranteed |
| Public | Nodes may be run by any party | High | High | Guaranteed |

Source: Authors

of loss, tampering or damage to the bill of lading have been reduced to near-zero. Also according to [13], cost of issuance has been reduced to approximately 15% of the estimated usual price for sending paper document through courier services.

Audit company Deloitte signed a partnership with the Norwegian certification company DNV GL [14]. They transferred all its 90 000 certificates to a private blockchain. In addition, acts on technical inspections of ships and oil installations were transferred to a private blockchain since such documents can be faked and tampered with. BT block counterfeit certificates, allowing maritime industry to manage their certification in a transparent and secure way.

Cyber attacks against COSCO and ransomware breach against Maersk in 2018, proved that more effort is needed to defend against cyber incidents [15]. Author pointed that blockchain should be considered as effective protection against unauthorized data tampering and could be used as a deterrent against cyber threats. He also mentioned that ship owners and vessel operators are more occupied with environmental compliance than pursuing investments in the technology.

### Authentication using BT

Increasing cases of identity thefts and data leaks makes authentication a major concern. Most internet application systems e.g. (email system, messaging application systems and websites) are based on central authority technique which issues and activates certificates, and store all the data [8]. This approach pose a fatal security risk since bad actors or hackers could attack the central authority, steal or counterfeit user's identity or crack encrypted information.

Identity authentication system based on blockchain with its decentralized characteristics doesn't challenge existing central institutions or authority's. Moving central authority role, from providing data storage for identity verification, to verifier of user's identity, improves the security of authentication system since no data is stored. This type of identity authentication system is already used, Estonian citizen and e-residents are issued with a cryptographically secure digital identification card based on BT on the backend, granting access to various public services [16].

### BT as storage network

Storing data on a single host (trusted or untrusted) doesn't guarantee availability, bandwidth or general of quality service. Component failure is a guarantee, servers providing network access to hard drives where data is stored will also fail, network links may collapse and storage may become unreliable. So, data must be stored with enough redundancy to recover from these failures.

We propose storing data across multiple hosts on a decentralized network. On this type of network, data files are broken apart and spread over multiple hosts in a process called sharding [17]. Also, data is encrypted with a private key which makes it secure and tamper proof.

On network made by [17], hosts prove their storage by providing a segment of the original file and list of hashes from file's Merkle tree, this information is sufficient to prove that segment came from original file. Thus, since proofs are written on the blockchain, anyone can verify their validity or invalidity [17]. Storage host's are awarded for every proof they submit, and are penalized for missing proofs. Data encryption protects privacy of data and any tampering will be identified. Authorized users will be able to edit, add and remove files.

### Proposed scheme for Autonomous Vessels Control

Usage of BT for autonomous vessels control is proposed and illustrated in Fig. 2. Vessels' control data and essential ship data are sharded and stored on distributed consensus network and can be accessed only by certified user. Every new user has to pass through Certification Authority (CA) before accessing the network. CA is core of authentication system. Its role is to verify users' identity, issue, update, revoke or confirm certificates. Cryptographically secure digital identification certificates are issued to all certified users. This approach removes threat of bad actors tampering with the data or stealing sensitive data.



Journal of Applied Engineering Science Vol. 17, No. 3, 2019
ISSN 1451-4117

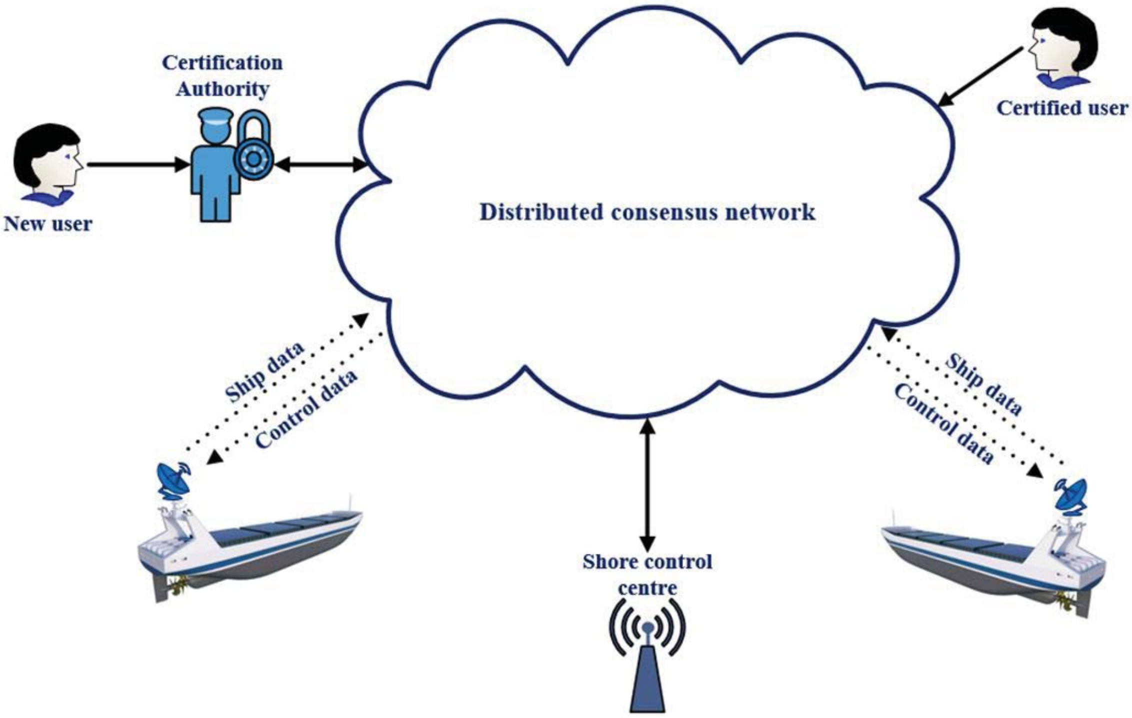


*Figure 2: Proposed usage of the BT for autonomous vessels control*
*Source: Authors*

## CONCLUSION

This paper considers blockchain technology as improvement in security of communications and data security for MASS. Scheme for implementation is proposed that eliminates some threats for MASS communication systems. Since blockchain technology is already making its way into industry, its benefits in field of secure authentication should be used in maritime industry. This scheme makes unauthorized access blocked at start and easily detectable. Storing data on distributed consensus network ensure only authorized users can access the content. Blockchain technology is already introduced to maritime industry in form of bill of lading, regulation compliance, etc. and is expected to bring significant cost-saving opportunities in the industry. This technology shows a great potential for researches and investigations in both science and technology and it is a desire that this paper will be of use in further development of technology projects in this field.

## REFERENCES

1. Rolls-Royce. Finferries and Rolls-Royce test fully autonomous ferry in Finland, from: https://www.ship-technology.com/news/finferries-rolls-royce-ferry/, accessed on 2019-07-07
2. Höyhtyä, M., Huusko, J., Kiviranta, M. (2017). Connectivity for Autonomous Ships: Architecture, Use Cases, and Research Challenges, 2017 International Conference on Information and Communication Technology Convergence (ICTC), 18-20 Oct. 2017, Jeju, South Korea, p. 345 - 350
3. Mraković, I., Vojinović, R. (2019), Maritime Cyber Security Analysis – How to Reduce Threats? Transactions on Maritime Science 8(1), p. 132-139.
4. Rødseth, Ø. J., Nordahl, H. (2017), Definition for Autonomous Merchant Ships, Norwegian Forum for Autonomus Ships, from http://nfas.autonomous-ship.org/resources/autonom-defs.pdf, acessed on 2019-08-07
5. Managed, I. S., Thomas, B. Y. The human element, UK P & I CLUB, no. 1–8.
6. Maritime Unmanned Navigation through Intelligence in Networks, from http://www.unmanned-ship.org/munin/, accessed on 2019-09-07
7. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, Archive, from https://bitcoin.org/bitcoin.pdf, accessed on 2019-06-07
8. Liu, L., Xu, B. (2018). Research on Information Security Technology Based on Blockchain, IEEE 3rd International Conference on Cloud Computing and Big Data Analysis, 20-22 April 2018, Chengdu, China, 380-384.
9. Swan, M. (2015), Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol, Calif.
10. Wingrove, M. Ten technologies to shake up maritime in 2018, from https://www.marinemec.com/news/view,ten-technologies-to-shake-up-maritime-in-2018_50317.htm, accessed on 2019-08-07
11. Consortium to build global shipping blockchain, Digital Ship, Dec 2018 / Jan 2019, pp. 13

12. Li, C. Maersk – Reinventing the Shipping Industry Using IoT and Blockchain, from https://digital.hbs.edu/industry-4-0/maersk-reinventing-shipping-industry-using-iot-blockchain/, accessed on 2019-09-07
13. MI News Network. First Ever Blockchain-Based CargoX Smart B/I Successfully Completed its Historic Mission, from https://www.marineinsight.com/shipping-news/first-ever-blockchain-based-cargox-smart-b-l-successfully-completed-its-historic-mission/, accessed on 2019-19-08
14. DNV GL. Deloitte and DNV GL deliver the first blockchain solution in the certification industry, from www2.deloitte.com/ie/en/pages/about-deloitte/articles/Deloitte_DNV_GL_first_ blockchain_solution_certification_industry.html, accessed on 2019-10-07
15. Gallagher, J. COSCO fleet could still be at risk following attack, warns cyber expert, from https://safetyatsea.net/news/2018/cosco-fleet-could-still-be-at-risk-following-attack-warns-cyber-expert/, accessed on 2019-19-08
16. Korjus, K. Estonian President Kersti Kaljulaid reveals the future direction of e-Residency, from https://medium.com/e-residency-blog/estonian-president-kersti-kaljulaid-reveals-the-future-direction-of-e-residency-5b1177dfa78c, accessed on 2019-14-07
17. Vorick, D., Champine, L., Nebulous Inc. (2014). Sia: Simple Decentralized Storage, from https://sia.tech/sia.pdf, accessed on 2019-17-07

*Paper submitted: 03.07.2019.*
*Paper accepted: 21.08.2019.*