ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 3 (2), 2023

https://doi.org/10.23939/ictee2023.02.

DIGITAL ENTITIES COMMUNICATION WITHIN A BLOCKCHAIN-ENABLED INTELLIGENT TRANSPORT SYSTEM

Y. Babich [ORCID: 0000-0002-7888-7591], D. Bagachuk [ORCID: 0000-0001-8798-891X], L. Bukata [ORCID: 0000-0003-1707-1633], L. Hlazunova, S. Shnaider

State University of Intellectual Technologies and Telecommunications, 1, Kuznechna str., Odesa, 65023, Ukraine

Corresponding author: Y. Babich (e-mail: babich159@gmail.com)

(Received 20 June 2023)

Nowadays the blockchain is considered to be an integral part of intelligent transport systems. Intelligence of a transport systems allows to increase road safety, wisely utilize systems' resources and provide additional services to participants. However, blockchain implementations for intelligent transport systems must be adopted to the peculiarities of such systems. This work analyzes existing blockchain solutions, their features, advantages, drawbacks, and presents a consortium type blockchain implementation for an intelligent transport system. This implementation includes a two-layered architecture of digital entities interaction, consideration for digital entities distribution over the layers, consensus mechanism selection and its implementation, trust model considerations, and a block structure for the proposed blockchain implementation. The article also brings the solution to the single point of failure vulnerability of the proposed blockchain system. Thus, the paper covers key aspects of a blockchain design for an intelligent transport system.

Key words: *intelligent transport system, consortium blockchain, digital entity.*
UDC: 004.75, 004.72.

1. Introduction

Transport systems always used to develop with the focus on safety and smart resources utilization. However, recent past decades brought unprecedented opportunities enabling an intelligent transport system through Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and finally Vehicle-to-Everything (V2X) communications. intelligent transport system (ITS) is a transport system where vehicles, road facilities, and authorities are capable of interacting with each other in order to maximize degree of system's resources utilization and ensure traffic safety. Despite the fact that in this paper an ITS, its purpose, and main components are understood as they are defined in [1] and [2], we use a general term of digital entity for a vehicle, a roadside unit (RSU), or any other ITS component capable of real-time interactions, because we expect the variety of such components to grow over time. Interaction within a smart transport system requires robust mechanism that guaranties traceability, sustainability, ability to withstand substitution attacks. All these requirements can be met by using a blockchain technology.

Blockchain technology is widely used in the financial sector and has become widely known due to the popularity of cryptocurrencies. Features of blockchain allow this technology to be applied in other areas. For example, it is applied in royalty and copyright tracking systems, voting systems, logistics, healthcare etc. Thus, according to [3], the global blockchain in retail market size was valued at USD 240.45 million in 2022 and is projected to reach USD 30,641.76 million by 2030.

The White Paper [4] of the International Economic Forum points out the following advantages of the blockchain technology used in the transport sector: traceability and impossibility of information substitution, distribution, automation through smart contracts, increased speed, transparency, efficiency and security, the ability to provide new services.

Such features of the blockchain technology as the decentralized nature, traceability and the impossibility of substituting information made it an integral part of an ITS [5, 2]. However, we strongly agree to the point, expressed in [6], that adoption of an existing blockchain (like the one for cryptocurrencies or others mentioned in [3]) is not directly applicable for interaction of digital entities within an ITS.

The task of this work is to design a scalable blockchain-based architecture of digital entities interaction suitable for an ITS. This task contributes to the global problem of blockchain-enabled ITS synthesis, which, in turn, contributes to road safety and smart utilization of ITS resources.

In addition to the mentioned above features of the blockchain technology, it is necessary to highlight the ability of the blockchain to create a trusted environment with the controlled degree of anonymity. This exact property is used to solve the task formulated above.

We propose to use a digital entity trustworthiness in the combination with a controlled degree of anonymity as the basis for the digital entities interaction architecture within a blockchain-enabled ITS.

The set above task can be decomposed into several subtasks including:

1) determination of layers' quantity for the communication architecture and the principle of digital entities distribution all over the layers;
2) selection of a consensus mechanism suitable for the architecture;
3) design of a block for the blockchain implementation.

2. Related works

Being decentralized by its nature, the blockchain integrated to an ITS contrasts with the structure of the transport system that is centralized to some extent (in terms of management, data storage, road information spread).

Blockchain system can be one of the three types: public, private, or consortium [7]. Authors of the works [6, 8] present decentralized and public blockchain solutions for an ITS. The work [2] states that implementation of the blockchain eliminates centralization in an ITS and vehicles are equally responsible for making decisions with the help of V2X. Decentralization allows to eliminate a single point of failure [6, 7, 2], i.e. if a central node is compromised or damaged system can not function, which is not the case if the system is decentralized, because there is no central node. It is also worth noticing that public decentralized blockchain implementation allows to preserve privacy of an entity within ITS. However, privacy of an entity within ITS can also be preserved in the case of private or consortium blockchain [9, 10, 11].

The ability of blockchain to create a trusted environment led to trustworthiness researches. According to [6] a trust model can be either entity based, data-centric based or hybrid. Authors of the work [12] propose the entity based trust model relying on an entity reputation. The paper [13] presents the approach to messages trustworthiness estimation.

We propose a blockchain implementation of the consortium type, i.e. partially decentralized, selectively permissioned consensus (only the entities predefined by an ITS administration (or administrations) participate in the consensus), data access is available for all the entities. This approach allows to harmonize decentralized blockchain and centralized (to some extent) transport system. It also ensures very high mining efficiency, which in the case of the blockchain-enabled ITS (BEITS) is the ability to generate blocks containing transactions (messages). However, such a blockchain implementation for the ITS is potentially vulnerable to a single point failure problem and weaker data immutability. The ways to mitigate the mentioned vulnerabilities are known and presented in the following chapters.

The digital entities predefined to participate the consensus are considered to be trustworthy, while other digital entities must be examined for entity and information trustworthiness. Thus, the proposed system uses a hybrid trust model.

3. Architecture of digital entities communications within a BEITS

In this work a term of digital entity refers to any vehicle or a road facility capable of interacting with others in order to harmonize traffic and improve road safety.

Interaction between digital entities is aimed at spreading information about road conditions, traffic hazards, and general harmonization of traffic, as well it allows to predict behavior of a digital entity in order to optimize usage of available resources of the ITS.

Every digital entity can be characterized by a set of attributes

$$A_O = \{a_1, a_2, \ldots, a_n\}, \text{ and } n \in N. \quad (1)$$

Digital entities differ from each other with the set of attributes they have. New types of the ITS participants (drones, for example) that may appear in the foreseeable future will differ from existing vehicles or RSUs with their attributes sets.

Every digital entity (DE) consumes a set of services

$$S_O = \{s_1, s_2, \ldots, s_n\}, \text{ where } n \in N. \quad (2)$$

The services provided by the ITS are listed in [2] and include intelligent routing and navigation, preventing traffic jams; early warnings about road hazards; driver or vehicle support services, such as fines for violation of road laws; entertainment for onboard users, such as streaming media; providing statistical data about the surrounding areas, traffic, and environment.

At the same time, any digital entity has a set of identifiers

$$I_O = \{i_1, i_2, \ldots, i_n\}, \text{ where } n \in N. \quad (3)$$

In the consortium blockchain implementation we propose, identifiers are only exposed to the digital entities involved in the consensus.

Operational environment of a smart transport system uniting digital entities can be described with the following set of parameters

$$E_O = \{e_1, e_2, \ldots, e_n\}, \text{ where } n \in N. \quad (4)$$

These are required to identify road hazards, malfunctions of road facilities, etc.

Probability of adding a block to the blockchain by a single digital entity can be expressed as

$$P_B = f(I_O, S_O, E_O). \quad (5)$$

The decision about adding a block to the blockchain is made through the consensus between the digital entities predefined by the ITS administration. Parameters (1)–(4) involved in consensus are included in a smart contract that is a part of the blockchain.

Consortium type of the proposed blockchain means that not all the DEs are involved in the consensus. Only the ones predefined by the ITS administration do. Thus, we propose a two-layered architecture, where the DEs involved in the consensus are at the second layer, while all the rest are at the first.

Fig. 1 shows the 2-layered architecture of DEs interaction for the proposed consortium blockchain. In a transport environment not all the elements have the same priority. This logic is reflected by the proposed blockchain architecture. However, the parameter of inequality here is trust instead of priority. DEs of the second layer are more trusted than the ones from the first layer.

There is no need to add more layers to the architecture, because here we have only two groups of DEs. Any DE of the given system can generate a block. However, only the DEs of the second layer participate the consensus and make a decision on whether the block is added or declined. All the DEs have the (1)–(4) characteristics, while only the DEs of the second layer use policies and rating system to calculate the probability (5).

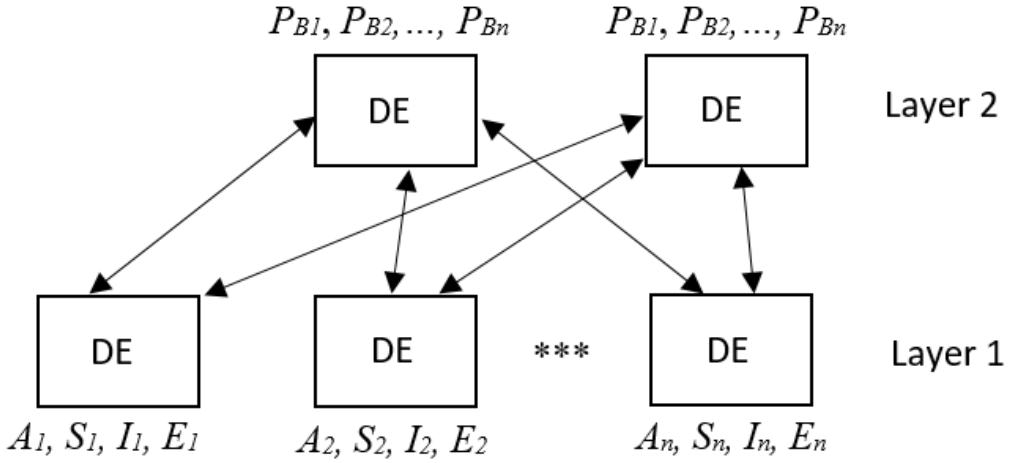

Fig. 1. Architecture of the digital entities interaction

The proposed architecture also guaranties partial anonymity, because DEs of the first layer expose their identity to the second layer DEs but not to each other.

The single point of failure vulnerability can be mitigated through the quantity of the second level DEs.

It should be mentioned that the architecture shown in the Fig. 1 is fair for the case of adding a block to the blockchain, while DEs still can interact horizontally (for example, the second layer DEs during consensus).

Considering operation environment of a smart transport system, it is possible to assume presence of intruders or other entities willing to harm or destabilize the system. This actualizes the task of digital entity behavior prediction. This task can be solved by using a rating system and policies enforced by the second level DEs.

Considering the task of selecting a consensus mechanism to be implemented, the scaling must be considered at the first place, because the ITS is a large system and it must not be flooded with excessive service data and must maintain its functionality if some of the second layer DEs are compromised or malfunction.

4. Consensus mechanism

Since we propose a consortium type blockchain, let us examine consensus mechanisms for both – public and private blockchains.

The following mechanisms are examining worthy: Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Capacity, Proof of Elapsed Time, Proof of Activity, Proof of Weight, Proof of Importance. These consensus mechanisms are described in the sources [14–22].

Let us use the method of a criteria weighted sum to find the best suitable consensus mechanism for the proposed blockchain implementation for the ITS. The criteria to be considered are support of hierarchy (since we have the 2-layered architecture) and scalability (in terms of excessive traffic generation). The weight coefficients are 0.7 and 0.3 respectively.

The consensus mechanisms and their scores are given in the Table 1.

According to the scores given in the Table 1, the most suitable consensus mechanism for a proposed system is the Proof of Authority (PoA). The runner up is the Proof of Weight. Both of these consensus mechanisms proofed their efficiency in a permissioned environment, where digital entities are not completely anonymous.

Table 1

Consensus mechanisms and their scores

No.	Mechanism	Hierarchy support	Scalability	Weighted sum
1	Proof of Work	0	9	2.7
2	Proof of Stake	6	8	6.6
3	Proof of Authority	10	5	8.5
4	Proof of Burn	5	7	5.6
5	Proof of Capacity	0	7	2.1
6	Proof of Elapsed Time	2	7	3.5
7	Proof of Activity	5	7	5.6
8	Proof of Weight	7	6	6.7
9	Proof of Importance	3	6	3.9

However, according to the work [16], PoA algorithms are not actually suitable for permissioned blockchains deployed over the Internet, which is likely to be the case of an ITS, because of wide geographical distribution. In this case, the work [16] advocates the Practical Byzantine Fault Tolerance (PBFT) algorithm [23] as the better choice in terms of consistency. Such a change is acceptable, since PoA belongs to the family of BFT algorithms. Thus, the proposed solution will use the PBFT-based consensus mechanism. PBFT allows to maintain functionality unless quantity of compromised or malfunction DEs of second layer stays under 1/3. Implementation of PBFT also allows to strengthen data immutability, because an attacker has to compromise 1/3 of the second layer DEs before substituting data.

5. Block structure

We propose the following block structure for the consortium type blockchain implementation for the ITS. General principles of a block structuring could be found in [24].

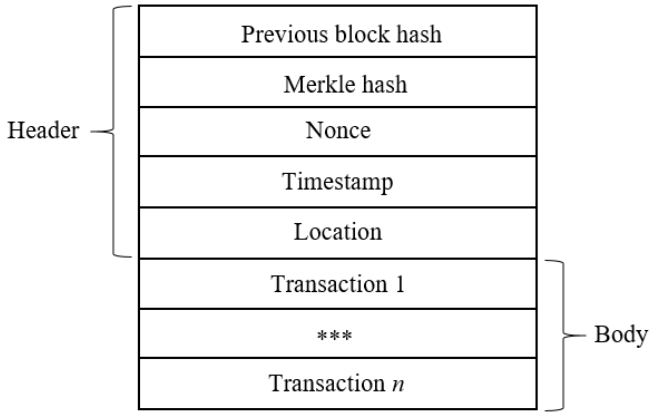

Fig. 2. Block structure

The proposed block format includes a header and a body. Previous block hash field contains corresponding hash to maintain blockchain integrity. Size of this field is 32 bytes. Merkle hash is required for data immutability and hashes all transactions of the block. The Merkle hash is calculated by means of the Merkle algorithm [25]. Size of this field is 32 bytes. The nonce field takes 4 bytes. Since the blockchain for the ITS has an event-driven logic of blocks generation, we added a Timestamp field of 4 bytes. Considering the fact that DEs are highly mobile within the ITS, we also added the location field, that is 8 bytes in length. Thus, the header takes 80 bytes, which is comparable to the block structure proposed by the authors of [6]. The body of the block contains arbitrary number of transactions, i.e. messages. Typical messages include navigation messages, assistance requests, emergency reports, and position beacons.

It must be noticed, that digital entity identifiers (3) are a part of a transaction but not a header. Messages structures are the subject of the further research and will be presented in the oncoming works.

Conclusion

The existing blockchain implementations (like the ones for cryptocurrencies) can not be straightly adopted for an intelligent transport system. They have to be modified in order to consider the ITS peculiarities including high mobility of units and their variety, different priorities and responsibilities, some extent of centralization.

This work presents a consortium type blockchain implementation for an intelligent transport system. This implementation includes a two-layered architecture of digital entities interaction, the PBFT-based consensus mechanism, which mitigates the single point of failure vulnerability and strengthens data immutability. The work also presents a block structure for the blockchain implementation suitable for the intelligent transport system. The block has an 80-byte header and variable part containing transactions generated by a digital entity.

The proposed consortium type blockchain implementation enables partial anonymity, because digital entities of the first layer keep anonymity to each other but expose their credentials to the digital entities of the second layer of the architecture.

From the trust model point of view, the second layer digital entities are considered to be trustworthy, while the digital entities at the first layer are the subject of entity and information trustworthiness checks. Thus, the proposed solution uses a hybrid trust model.

Combination of all the mentioned features of the proposed blockchain implementation, i.e. the two-layered architecture of digital entities interaction, the PBFT-based consensus mechanism, the proposed block structure, partial anonymity, the hybrid trust model forms to the novelty of the proposed solution and differs it from the existing ones.

Also purpose of this paper is to stimulate scientific discussions and further research of the private and consortium type blockchain implementations for intelligent transport systems and peculiarities of such blockchains.

References

[1] *Meneguette, R., De Grande, R., Loureiro, A. (2018). Intelligent Transport System in Smart Cities. Aspects and Challenges of Vehicular Networks and Cloud, p. 182. DOI: 10.1007/978-3-319-93332-0.*

[2] *Waseem, M., Ahmed, K., Azeem, M. (2021). Blockchain Based Intelligent Transport System. Modern Innovations, Systems and Technologies, 1(3), pp. 70–88. DOI: 10.47813/2782-2818-2021-1-3-70-88.*

[3] *Blockchain In Retail Market Sales, Demand Outlook by Component, Type, Application & Region – Forecast 2023 – 2030. Contrive Datum Insights. Available at https://www.contrivedatuminsights.com/product-report/blockchain-in-retail-market-248372/?Mode=PM*

[4] *Building Value with Blockchain Technology:How to Evaluate Blockchain's Benefits. World Economic Forum White Paper. Available at http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf*

[5] *Nam, K., Dutt, C., Chathoth, P., Khan, M. (2021). Blockchain technology for smart city and smart tourism: latest trends and challenges. Asia Pacific Journal of Tourism Research, Vol. 26, No. 4, pp. 454–468. DOI: 10.1080/10941665.2019.1585376*

[6] *Shrestha, R., Bajracharya, R., Shrestha, A., Nam, S. (2020). A new type of blockchain for secure message exchange in VANET. Digital Communications and Networks, Vol. 6, Iss. 2, pp. 177–186. DOI: 10.1016/j.dcan.2019.04.003.*

[7] *Jabbar, R., Dhib, E., Ben Said, A., Krichen, M., Zaidan, E., Barkaoui, K. (2022). Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. IEEE Access, Vol. 10, pp. 20995–21031. DOI: 10.1109/ACCESS.2022.3149958.*

[8] Hou, J., Ding, W., Liang, X., Zhu, F., Yuan, Y., Wang, F. (2021). A Study on Decentralized Autonomous Organizations Based Intelligent Transportation System enabled by Blockchain and Smart Contract, 2021 China Automation Congress (CAC), Beijing, China, pp. 967–971. DOI: 10.1109/CAC53003.2021.9727429.

[9] Zhang, X., Chen, X. (2019) Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. IEEE Access, Vol. 7, pp. 58241–58254. DOI: 0.1109/ACCESS.2018.2890736.

[10] Lu, Z., Liu, W., Wang, Q., Qu, G., Liu, Z. (2018) A privacy-preserving trust model based on blockchain for VANETs. IEEE Access, Vol. 6, pp. 45655–45664. DOI: 10.1109/ACCESS.2018.2864189.

[11] Zheng, D., Jing, C., Guo, R., Gao, S., Wang L. (2019) A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access, Vol. 7, pp. 117716–117726. DOI: 10.1109/ACCESS.2019.2936575.

[12] Marmol, F., Martinez, G. (2011). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer, Vol. 35 (3), pp. 934–941. DOI: 10.1016/j.jnca.2011.03.028.

[13] Gurung, S., Lin, D., Squicciarini, A., Bertino, E. (2013). Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks. Network and System Security, Vol. 7873, pp. 94–108. DOI: 10.1007/978-3-642-38631-2_8.

[14] Jakobsson, M., Juels, A. (1999). "Proofs of Work and Bread Pudding Protocols". Secure Information Networks: Communications and Multimedia Security. Kluwer Academic Publishers, pp. 258–272. DOI: 10.1007/978-0-387-35568-9_18.

[15] Bentov, I., Gabizon, A., Mizrahi, A. (2016). Cryptocurrencies Without Proof of Work. Financial Cryptography and Data Security, Vol. 9604, pp. 142–157. DOI: 10.1007/978-3-662-53357-4_10

[16] De Angelis, S., Aniello, L., Lombardi, F., Margheri, A., Sassone, V. (2017). PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. Available at https://www.researchgate.net/publication/320619309_PBFT_vs_proof-of-authority_applying_the_CAP_theorem_to_permissioned_blockchain

[17] P4Titan (2014) Slimcoin A Peer-to-Peer Crypto-Currency with Proof-of-Burn Available at https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf

[18] Dziembowski, S., Faust, S., Kolmogorov, V., Pietrzak, K. (2013). Proofs of Space. Available at https://eprint.iacr.org/2013/796.pdf

[19] Curran, B. (2018) What is Proof of Elapsed Time Consensus? (PoET) Complete Beginner's Guide. Avail-able at https://blockonomi.com/proof-of-elapsed-time-consensus/

[20] Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. ACM SIGMETRICS Performance Evaluation Review, Vol. 42, Iss. 3, pp. 34–37. DOI: 10.1145/2695533.2695545

[21] Chen, J., Micali, S. (2019). Algorand: A secure and efficient distributed ledger Available at https://www3.cs.stonybrook.edu/~jingchen/papers/Algorand_A%20secure%20and%20efficient%20distributed%20ledger_TCS.pdf. DOI: 10.1016/j.tcs.2019.02.001

[22] NEM Technical Reference. Version 1.2.1 (2018) Available at https://nemproject.github.io/nem-docs/pages/Whitepapers/NEM_techRef.pdf

[23] Castro, M., Liskov, B. Practical Byzantine Fault tolerance (2002) Proc. Third Symposium on Operating Systems Design and Implementation, p. 114.

[24] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash. Bitcoin: a peer-to-peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

[25] Merkle, R. (1987). A digital signature based on a conventional encryption function. Proceedings of CRYPTO 1987, pp. 369–378. DOI: 10.1007/3-540-48184-2_32.

КОМУНІКАЦІЯ ЦИФРОВИХ ОБ′ЄКТІВ У ІНТЕЛЕКТУАЛЬНІЙ ТРАНСПОРТНІЙ СИСТЕМІ З ПІДТРИМКОЮ БЛОКЧЕЙНУ

Ю. Бабіч, Д. Багачук, Л. Буката, Л. Глазунова, С. Шнайдер

Державний університет інтелектуальних технологій і зв'язку, вул. Кузнечна, 1, Одеса, 65023, Україна

Сьогодні блокчейн вважається невід'ємною частиною інтелектуальних транспортних систем. Інтелектуальність транспортних систем дає змогу підвищити безпеку дорожнього руху, раціонально використовувати ресурси систем і надавати додаткові послуги учасникам. Однак реалізації блокчейну для інтелектуальних транспортних систем необхідно адаптувати до особливостей таких систем. У роботі проаналізовано відомі блокчейн-рішення, їх особливості, переваги та недоліки, а також наведено реалізацію блокчейну консорціумного типу для інтелектуальної транспортної системи. Ця реалізація передбачає дворівневу архітектуру взаємодії цифрових об'єктів, розгляд розподілу цифрових об'єктів за рівнями, вибір механізму консенсусу та його реалізацію, міркування стосовно моделі довіри та структуру блоків для запропонованої реалізації блокчейну. У статті також подано рішення для вразливості типу "єдина точка відмови" запропонованої системи блокчейн. Отже, стаття охоплює ключові аспекти синтезу блокчейну для інтелектуальної транспортної системи.

Ключові слова: *інтелектуальна транспортна система; консорціумний блокчейн; цифрова сутність.*