COMPUTATIONAL PROBLEMS OF ELECTRICAL ENGINEERING

Vol. 14, No. 2, 2024

TYPES OF MESSAGES FOR A BLOCKCHAIN-ENABLED INTELLIGENT TRANSPORT SYSTEM

Iryna Tregubova, Yurii Babich

State University of Intellectual Technologies and Telecommunications, Odesa, Ukraine

y.o_babich@suitt.edu.ua

https://doi.org/10.23939/jcpee2024.02.022

Abstract: This work continues the topic of blockchain-enabled intelligent transport system design and focuses on groups of messages (transactions) suitable for such a system. Precisely, the work proposes to extend the known set of messages with two new groups – traffic optimization messages and commercial offers / requests. The messages of the first group allow the implementation of traffic optimization tools based on artificial intelligence and other traffic forecasting tools available for an intelligent transport system. For example, it is possible to increase efficiency of intelligent transport system throughput utilization by instructing a driver to slow down, speed up or to take a detour route when necessary. At the same time messages of the second group (commercial offers / requests) contribute to road safety through making vehicles maintenance services available intime. The combination of a two-layer architecture for the interaction of digital entities, the PBFT-based consensus mechanism, elaborated block structure and the messages disclosed in this work contribute to the scientific novelty and uniqueness of the proposed blockchain implementation for an intelligent transport system.

Key words: intelligent transport system, consortium blockchain, types of transactions.

1. Introduction

Within this paper an intelligent transport system is understood as 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], the work [3] introduces a general term of Digital Entity (DE) for a vehicle, a roadside unit (RSU), or any other ITS component capable of real-time interactions along with an architecture of such interaction thst is shown in Fig. 1.

Precisely, article [3] proposes a consortium type blockchain implementation for an intelligent transport system. This implementation includes a two-layered architecture of digital entities interaction, a PBFT-based [4] consensus mechanism, which mitigates the single point of failure vulnerability and strengthens data immutability.

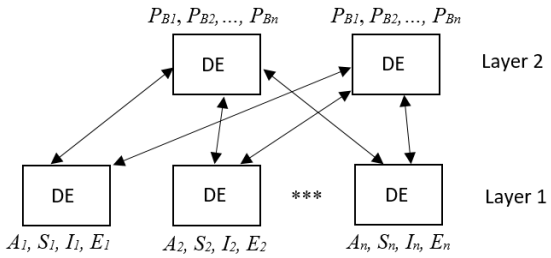

Fig. 1. Architecture of the digital entities interaction.

The work [3] also contributes to and supports the point, expressed in [5], that the adoption of an existing blockchain is not directly applicable to the interaction of digital entities within an ITS. Therefore, [3] proposes its own implementation of a consortium type blockchain for an intelligent transport system.

However, the work [3] does not include exact types of messages or their general groups for implementing within the proposed consortium type blockchain implementation for an intelligent transport system.

The objective of this study is to disclose the general groups of messages that are suitable for the consortium type blockchain proposed in [3], as well as exact messages that belong to these groups. This task contributes to the global problem of blockchain-enabled ITS synthesis, which, in turn, contributes to enhancing road safety and optimizing the utilization of ITS resources.

The aforementioned task can be subdivided into the following subtasks: a) an analysis of extant solutions for groups / messages within blockchain-enabled ITS; b) A disclosure of general groups of messages suitable for the consortium type blockchain implementation for an ITS proposed in [3]; and c) a disclosure of exact messages belonging to the groups mentioned above.

2. Related works

The general concept of an ITS has been thoroughly examined and described in detail.

The work [6] postulates the accelerated development of Intelligent Transportation Systems. This has made reliable, real-time data transmission very important. The authors of [7] claim that implementing a blockchain makes ITSs more reliable and robust.

The works [8, 9] also observe the development of ITS and highlight new challenges that arise as a result of this development. This contributes to relevance of the topic of ITS enhancement.

The idea of applying blockchain to create a trusted environment in ITS is strongly supported, which leads to trustworthiness research [10, 5, 11]. Paper [10] introduces a blockchain-based authentication framework that relies on the Proof of Trust consensus mechanism to avoid redundant re-authentication while minimizing computational and communication costs. According to [5] a trust model can be entity-based, data-centric based, or hybrid. In [11], the authors propose an entity-based trust model based on an entity's reputation.

Paper [3] proposes a consortium-type blockchain implementation, i.e. partially decentralized, selectively authorized consensus (only entities predefined by the ITS administration (or administrations) participate in the consensus), and access to data is available for all the entities. This approach allows for harmonization of a decentralized blockchain and a centralized (to some extent) transport system. Furtheremore, tt also ensures very high mining efficiency, which in the context of blockchain-enabled ITS (BEITS) signifies the capability to generate blocks containing transactions (messages).

DEs in Fig. 1 have the following characteristics: A is a set of attributes; S refers to a set of services available to a DE; I is a set of DE's identifiers; E refers to ITS environment operational parameters; P_B refers to the probability of adding a block to the blockchain by a single digital entity. The decision to add a block to the blockchain is made by consensus between the second-layer digital entities predefined by the ITS administration.

In [3], the use of the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism was also selected and justified. The PBFT enables the maintainance of functionality provided that the number of compromised or malfunction DEs of the second layer does not exceed 1/3. The PBFT implementation also allows for the strengthening of data immutability, since an attacker has to compromise 1/3 of the second layer DEs before substituting data.

In addition, work [3] also proposed a block structure for implementing a consortium-type blockchain for ITS. This block structure is given in Fig. 2.

The proposed block format [3] includes a header and a body. The header includes the following fields:

– previous block hash – 32 bytes;
– Merkle hash – 32 bytes;
– nonce – 4 bytes;
– timestamp – 4 bytes;
– location – 8 bytes.

Thus, the header takes 80 bytes, which is comparable to the existing solutions proposed for ITS, for example in work [5].

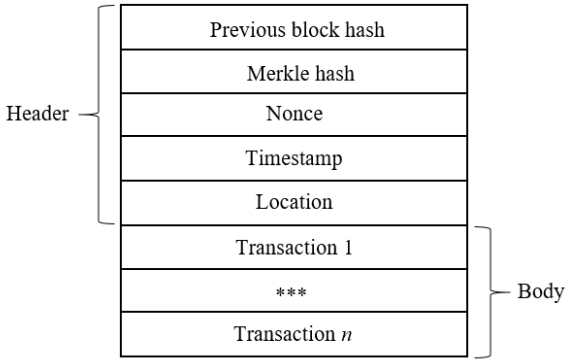

Fig. 2. Block structure.

The body of the block contains arbitrary number of transactions, i. e. messages. It is worth mentioning that digital entity identifiers I are included in transactions (messages) but not in a header.

3. Groups of messages to be exchanged within the BEITS

The subject of messages exchanged within blockchain-enabled ITS is the focus of ongoing research. For example, work [5] states that the main objective of ITS is to communicate with vehicles using messages to report safety-related events (including accident information, safety warnings, traffic congestion information, weather reports, messages regarding icy roads, etc.). The same authors summarize that there are two types of messages in ITS – beacon messages and safety-related event messages.

We propose to expand these groups of messages according to existing capabilities of a blockchain-enabled ITS. First of all, we refer to the traffic flow optimization capabilities provided by artificial intelligence and other predictive tools of a BEITS. This leads to the necessity to add a new group of messages – traffic optimization messages. These messages suggest tthat the driver slow down, speed up or take a detour. The main purpose of these messages is to maximize utilization of a BEITS throughput. Although the driver is expected to accept and follow the recommendation, the final decision is made by the individual driver.

Another group of messages that must be recommended for a BEITS is a group of messages containing commercial offers depending on a vehicle technical state or road conditions. For example, a message with the nearest oil or tire shop if a vehicle needs a corresponding service. Using this message group, a driver can access data or request some commercial services associated with road and traffic.

Let us summarize the proposed groups of messages to be exchanged within a BEITS in Fig. 3.

The proposed groups of transactions are distinguishing features of the proposed BEITS implementation.

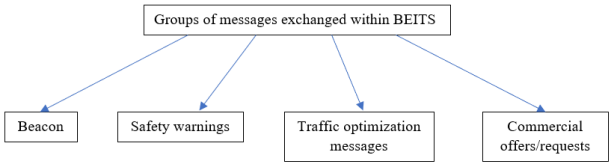

Fig. 3. Groups of messages exchanged within BEITS.

4. Messages exchanged within the BEITS

Let us start with the first group of messages – the beacon messages. This type of message is exchanged between a vehicle and an RSU in order to inform BEITS about vehicle's location. The format of a beacon message is given in Fig. 4.

MSG group	ID length	Vehicle ID
4	4	80 bits

Fig. 4. The beacon message

In Fig. 4, the MSG group field indicates a group of messages. This field takes 2 bits and in the case of a beacon is equal to "00". The ID length field takes 4 bits and specifies the length of the vehicle ID (which can be of variable length). At this stage of the project, we use the vehicle registration number as the vehicle ID within BEITS. Therefore, this field takes up to 80 bits, which allows for up to 10 ASCII encoded characters.

The next group of messages is the group of safety warning messages. The pattern of messages belonging to this group is shown in Fig. 5.

Messages belonging to the group of safety warnings are identified by a "01" value contained in the MSG group field. The origin field identifies a digital entity that originates this message. Typically, it is a second layer DE. However, a vehicle can be a source of this message if such a message passes through the PBFT consensus mechanism. The type field specifies a type of traffic hazard. Table 1 specifies the values of the type field and corresponding hazards.

MSG group	Origin	Type	Range	Description
4	80	4	10	560 bits

Fig. 5. Safety warning messages.

The range field of the message pattern specifies the radius in kilometers affected by the corresponding hazard. The center of the hazard is supposed to be shown in the location field of the block header (Fig. 2). The description field is used only in the case of an unspecified hazard to clarify it. This field can contain up to 70 ASCII encoded characters.

The range field of the message pattern specifies the radius in kilometers affected by the corresponding hazard. The center of the hazard is supposed to be shown in the location field of the block header (Fig. 2). The description field is used only in the case of an unspecified hazard to clarify it. This field can contain up to 70 ASCII encoded characters.

Table 1

Traffic hazards and their codes

MSG group	Traffic hazard	Code
01	Traffic accident	0000
01	Ice on the road	0001
01	Hurricane	0010
01	Fire	0011
01	Flood	0100
01	Snow blizzard	0101
01	Falling rocks	0110
01	Landslide	0111
01	Unspecified hazard	1000

Fig. 6 depicts a pattern of messages belonging to the group of traffic optimization messages.

MSG group	Origin	Destination ID	Rec type	Instructions
4	80	80	2	560 bits

Fig. 6. Traffic optimization messages

In the case of the messages shown in Fig. 6, the MSG group field contains a value of "10", which identifies messages belonging to this group. The origin field identifies the DE that is the source of the message. The destination ID field identifies the DE that is the destination of a message.

The recommendation type (Rec type) field encodes the exact recommendation given to the driver. At this stage of the project we consider the following recommendations: "Slow down" (00), "Speed up" (01) and "Take a detour" (10).

The Rec type field works in combination with the instructions field. In the case of the first two recommendations, it contains the recommended speed while in the case of the third recommendation, it contains details on the detour route.

The last group of messages for the BEITS is the group of commercial offers and requests. The pattern of the messages belonging to the group is given in Fig. 7.

MSG group	Origin	Destination ID	Offer/Request
4	80	80	1280 bits

Fig. 7. Commercial offers and requests.

The MSG group field of commercial offers and requests messages contains the combination of "11". The origin and destination ID field identify a sender and recipient of a particular message. The offer / request field

contains commercial offer for a vehicle or a request for a definite service (for example oil change or a tire service). This field can contain up to 160 ASCII encoded characters.

5. Conclusions

The scientific and engineering novelty of the proposed solution incorporates introduction of two additional groups of messages (transactions) in addition to the two already known groups available in existing solutions. The introduction of groups allows implementing traffic optimization tools based on artificial intelligence and other traffic forecasting tools available for ITS. It is expected that the introduction of a message group for the exchange of commercial offers and requests will increase road safety through the availability of intime vehicle maintenance services, as well as improve the driving experience.

The article also developes and discloses the message formats for existing groups (beacons and safety warning messages), which, in combination with the two-layer architecture of DEs interaction, the PBFT-based consensus mechanism, and the developed blockchain block structure, form a unique blockchain implementation for ITS.

References

[1] R. Meneguette, R. De Grande, end A. Loureiro, *Intelligent Transport System in Smart Cities. Aspects and Challenges of Vehicular Networks and Cloud*, Luxembourg: Springer Cham, 2018. https://doi.org/10.1007/978-3-319-93332-0

[2] K. Nam, C. Dutt, P. Chathoth, and M. Khan, "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, 2021. https://doi.org/10.1080/10941665.2019. 1585376

[3] Y. Babich, D. Bagachuk, L. Bukata, L. Hlazunova, and S. Shnaider, "Digital entities communication within a blockchain-enabled intelligent transport system", ICTEE, Lviv, Ukraine, vol. 3, No. 2, 2023. https://doi.org/10.23939/ictee2023.02.012

[4] M. Castro and B. Liskov, *Practical Byzantine Fault tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA, February 1999.

[5] R. Shrestha, R. Bajracharya, A. Shrestha, and S. Nam, „A new type of blockchain for secure message exchange in VANET", *Digital Communications and Networks*, vol. 6, No. 2, pp. 177–186, 2020. https://doi.org/10.1016/j.dcan.2019.04.003

[6] R. Mohandas, Y. Sudha, P. Narmatha, V. Prasad, and N. Manikandan, "Cognitive Congestion Alleviation Framework in IoT-Enabled WSN for Next-Gen Intelligent Transport Systems via Optimized Capsule Attention Network", *3rd International Conference on Intelligent Data Communication Technologies and Internet of Things*, Bengaluru, India, pp. 620–626, 2025. https://doi.org/10.1109/IDCIOT64235.2025. 10915117

[7] R. Jabbar, E. Dhib, A. Ben Said, M. Krichen, E. Zaidan, and K. Barkaoui, "Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review", IEEE Access, vol. 10, pp. 20995–21031, 2022. https://doi.org/10.1109/ ACCESS.2022.3149958

[8] S. Kaleem, M. Babar, B. Qureshi, M. EI-Affendi, and A. Koubaa, "Comparative Analysis of Federated Learning Techniques in Big Data-Driven Intelligent Transportation Systems", *8th International Conference on Data Science and Machine Learning Applications*, Riyadh, Saudi Arabia, pp. 126–131, 2025. https://doi.org/10.1109/CDMA61895.2025.00027

[9] C. Miranda, et al. "A Virtual Infrastructure Model Based on Data Reuse to Support Intelligent Transportation System Applications", *IEEE* Access, vol. 13, pp. 40607–40620, 2025. https://doi.org/ 10.1109/ACCESS.2025.3547160

[10] P. Surapaneni, S. Bojjagani and M. K. Khan, "DYNAMIC-TRUST: Blockchain-Enhanced Trust for Secure Vehicle Transitions in Intelligent Transport Systems", *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2025. https://doi.org/10.1109/TITS.2025.3545755

[11] F. Marmol and G. Martinez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", *Journal of Network and Computer*, vol. 35, No. 3, pp. 934–941, 2011. https://doi.org/10.1016/j.jnca.2011.03.028

ТИПИ ПОВІДОМЛЕНЬ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ТРАНСПОРТНОЇ СИСТЕМИ ІЗ ПІДТРИМКОЮ БЛОКЧЕЙНУ

Ірина Трегубова, Юрій Бабіч

Публікація продовжує тему проєктування інтелектуальної транспортної системи із підтримкою блокчейну. Увагу зосереджено на транзакціях, які підходять для інтелектуальної транспортної системи. Запропоновано розширити відомий набір повідомлень двома новими групами – повідомленнями для оптимізації трафіку та комерційними пропозиціями / запитами. Повідомлення першої групи дають змогу реалізувати засоби оптимізації трафіку на основі штучного інтелекту, доступні для інтелектуальної транспортної системи. Повідомлення другої групи сприяють безпеці дорожнього руху через надання послуг із технічного обслуговування транспортних засобів.

Поєднання дворівневої архітектури взаємодії цифрових об'єктів, механізму консенсусу на основі алгоритму PBFT, розробленої структури блока блокчейну та повідомлень, розкритих у цій роботі, зумовлює науково-технічну новизну та унікальність пропонованої реалізації блокчейну для інтелектуальної транспортної системи.

Iryna Tregubova – Associate Professor, PhD in Computer Science, Head of the Computer Science Department at State University of Intellectual Technologies and Telecommunications. Research interests include computer-generated imagery, computer aided design technologies. Scientific results are published in more than 45 scientific papers.

Yurii Babich – PhD, Senior Lecturer at the Software Engineering Department at State University of Intellectual Technologies and Telecommunications. Research interests include blockchain, machine learning techniques. Scientific results are published in more than 30 scientific papers.

Received: 28.03.2020, Accepted: 25.04.2020

ORCID ID: 0000-0003-2030-7678 (I. Tregubova)
ORCID ID: 0000-0002-7888-7591 (Yu. Babich)