Application of Blockchain Technology and Cryptography Methods to Ensure Economic Security in the Transportation of Crude Oil

Anatoly Makarov, Elena Pisarenko, Gennady Vorobyev

Pyatigorsk State University, Pyatigorsk, Russia

doi: https://doi.org/10.21467/abstracts.93.95

ABSTRACT

A large number of parties that, generally speaking, have different goals, can participate in the processes of production, loading and transportation of crude oil by tankers. This can lead to conflict situations, misunderstanding, disputes and disagreement in assessing the quantity and quality of transported oil, which threatens the economic security of the processes. To eliminate such shortcomings and guarantee the reliability and accuracy of the data on the transported oil, it is proposed to use blockchain technology using cryptography methods. The schemes described in the article allow to control all transactions carried out in the process of loading and transportation of oil and ensure that no unrecorded actions can be performed that can lead to changes in its quality or quantity.

Document management systems used in the registration of production, loading, transportation, as well as in the acceptance and control of crude oil, cannot completely guarantee the reliability of all data, since they do not have reliable protection against additions, falsifications, and replacement with other documents. In some cases there are questions about trust in documents and data in various parts of the chain from production to processing (Kazemiand Szmerekovsky, 2015, Lukoil, 2013). This problem can be completely solved using distributed registry technologies based on cryptography methods and peer-to-peer blockchain networks. Such a system ensures the transparency and reliability of all transaction data, i.e. any actions with oil on the way from the place of production to the place of processing during shipping. The expediency of using blockchain technologies is due to the fact that up to 60 owners of oil can change on its way from the producer to the final consumer. The same oil can often appear in more than 100 contracts, which can lead to many errors and even falsifications (Klepikov, 2017)

The scheme we offer for the formation of blocks of the internal blockchain and the external block of the external blockchain network is shown in Fig. 1.

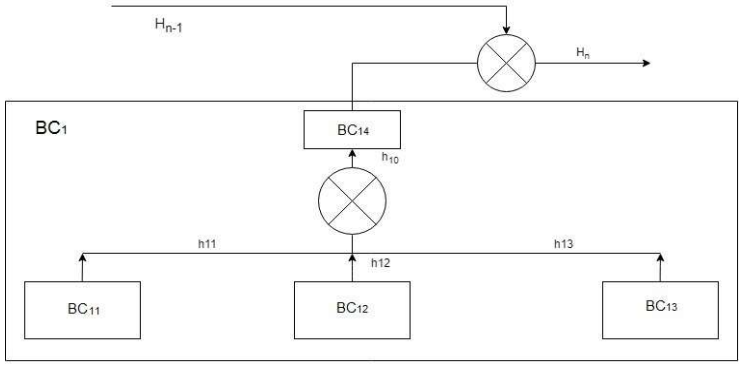

Fig. 1. The composition of the block of the internal blockchain with internal hashes in the external block of the network with a distributed registry

Designations in the figure:

BC_{11} – the block of data on the origin of crude oil and its geographical location;

BC_{12} – the block of the set of equipment used in the crude oil production;

BC_{13} – the block of equipment for measuring the main parameters of crude oil and data on its quantity when transferred to the next link;

DOI: 10.21467/abstracts.93

h_{11}, h_{12}, h_{13}, h_{10}, h_{14} – internal hashes of blocks BC_{11}, BC_{12}, BC_{13}, BC_{14};
h_{10} – the hash uniting blocks BC_{11}, BC_{12}, BC_{13};
h_{14} – the internal generalizing hashof block BC_{14};
h_n – the hash of final block BC_{14};
H_{n-1} – the external hash of the previous block;
H_n – the external hash number n of a new block of the network.
The scheme illustrates the formation of an internal block for embedding it in an external network block. The accuracy of the information is fixed by the corresponding hash, which immediately changes when any bit of the BC1, BC2, BC3 blocks is changed, and, most importantly, the filling of the primary space and the tanks of tanker is fixed. Thus, the task of tracking the origin of crude oil, as well as equipment involved in the processes of production, transportation and processing, is solved.
The scheme of the blocks of the external blockchain is shown in Fig. 2.

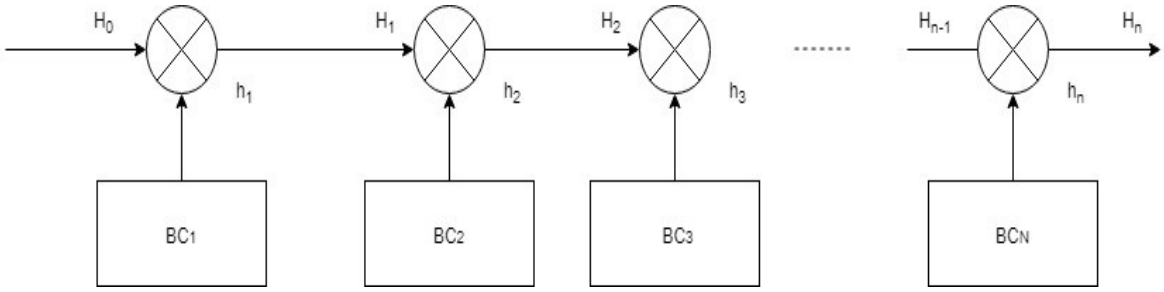

Fig. 2. An example of an external network for generating H_n hashes based on internal h_n

Thus, the data in the blocks are connected by hash functions and in order to change them in the next block, it is necessary to change the hash functions of all previous blocks, and this is almost impossible. The fact thateach network member has the entire database does not allow it to be destroyed or modified.
The considered schemes can be used as a basis for designing networks with a distributed registry (blockchain technologies) using cryptography methods to control all processes of crude oil tanker transportation.

References

Kazemi, Y., Szmerekovsky, J. Modeling downstream petroleum supply chain: The importance of multi-mode transportation to strategic planning (2015) *Transportation Research Part E: Logistics and Transportation* Review, 83, pp.111-125, www.elsevier.com/inca/publications/store/6/0/0/2/4/4/, doi: 10.1016/j.tre.2015.09.004

Global Trends in Oil and Gas Markets to 2025, 2017 (2013). http://www.lukoil.be/pdf/Trends_Global_Oil_ENG.pdf

Klepikov, V.P. Development of cargo flows and logistics infrastructure for the transportation of oil cargo in the South of Europe (2017) *Logistics and Supply Chain Management,* 3(80), pp.77-90.

DOI: 10.21467/abstracts.93