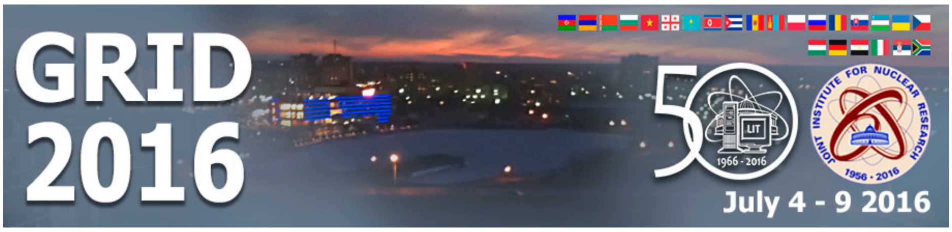
The 7th International Conference "Distributed Computing and Grid-technologies in Science and Education" (GRID 2016)



Contribution ID: **123** Type: **Sectional reports**

Security infrastructure for distributed computing systems on the basis of blockchain technology

Thursday 7 July 2016 16:30 (15 minutes)

To ensure secure access to resources of distributed computing systems (DCS) [1] with the account of rights of a given user and the service/resource policy, a security infrastructure is needed, which should be enough reliable and on the other hand not create significant difficulties for users. In the work [2], a method of user authentication, which is based on a login/password pair together with a session-restricted key was suggested. This approach provides a substantial simplification of both the registration of new users in the system and their operation in DCS, compared with the commonly used in DCS public key infrastructure (PKI) with the use of proxy certificates. However, a vulnerability area of both the PKI, and the solution proposed in [2], is the need of operation of a fail-proof and tamper-resistant central server in the security infrastructure. In the case of the infrastructure suggested in [2] this is the authentication/authorization server and in the case of PKI this is the server of proxy certificates renovation.

In this work, we investigate the possibility of abandoning the special dedicated servers in the DCS security infrastructure and the use instead of them a distributed database on the basis of the blockchain technology [3], the paradigm of smart contracts [4] and Ethereum protocol [5,6]. Since in this case the database of the security infrastructure is distributed across all the nodes in the system, this approach will increase the resiliency and security of DCS.

This work was supported by the Ministry of Science and Education of the Russian Federation, the Agreement No. 14.604.21.0146; unique identifier is RFMEFI60414X0146.

References
1. A. P. Kryukov, A. P. Demichev, and S. P. Polyakov, Web Platforms for Scientific Research, Programming and Computer Software, 2016, Vol. 42, No. 3, pp. 129–141
2. J. Dubenskaya, A. Kryukov, A. Demichev, N. Prikhodko, New security infrastructure model for distributed computing systems, Journal of Physics: Conference Series. 2016. Vol. 681, P. 012051-1-012051-5.
3. Public versus Private Blockchains , BitFury Group, 2015, http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf
4. N. Szabo, The Idea of Smart Contracts, http://szabo.best.vwh.net/smart_contracts_idea.html
5. V. Buterin, Ethereum White Paper, https://github.com/ethereum/wiki/wiki/White-Paper
6. G. Wood, Ethereum: A secure decentralised generalised transaction ledger, http://gavwood.com/paper.pdf

Author: Dr KRYUKOV, Alexander (SINP MSU)

Co-author: Dr DEMICHEV, Andrey (SINP MSU)

Presenter: Dr KRYUKOV, Alexander (SINP MSU)

Session Classification: 3. Middleware and services for production-quality infrastructures

Track Classification: 3. Middleware and services for production-quality infrastructures