UDC 004.01(082)

Suprun O., Savorona N.
Taras Shevchenko National University of Kyiv

DECENTRALIZED ELECTRONIC VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

Blockchain is a technology for organizing databases while ensuring its integrity and openness. The urgency of the implementation in voting system is determined by a number of reasons: there is no need to physically appear at polling stations and such system will have resistant to different cyber-attacks.

Creating the prototype, following architecture is taken as basis for decentralized anonymous voting system:

- Validators;
- User identification system;
- End users (voters).

Validator nodes process user transactions and reach consensus on a distributed database. User identification systems are required to provide information about user IDs that voters will use to authenticate themselves right to vote. The identification system can be both centralized and internal (or external) identity provider, as well as a distributed system identification and certification [1].

Java programming language was chosen as the basis of system. In proposed system, the consensus-building method is the proof-of-work. It's based on the requirement for the requesting party to perform some rather complex long-term work, the result of which is easily and quickly verified by the requesting party. This means that for adding a block to the chain, the creator needs to provide proof of the resource-intensive task. To simulate the work of the validator in the system, separate threads are created that are parallelly engaged in downloading the available in the system transactions, loading the block with transactions, which will be added to the Blockchain. In order to illustrate the work, certain restrictions have been added.

This approach allows validators to check whether the sender of the transaction has the right to vote. At the same time, a specific voter can be determined only by validators with a certain probability (the larger the size rings, the less probability is).

Used sources

1. Springall D. Security Analysis of the Estonian Internet Voting System / https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.