REPUBLIA

Technical competitive paper

INTRODUCTION

The large-scale development of blockchain technologies has a huge impact on the emergence of innovative projects and provides the world with real tools for both business and everyday life. However, such trends have negative consequences as well. Republia project, considering this, introduces a comparative analysis that includes system and platform analysis that are commonly used in the industry.

Republia is a global decentralized ecosystem that within a single project combines all the structural mechanisms and platforms able to meet user demand.
In addition, all subsystems are based on its own blockchain - Republia Blockchain, which is implemented using artificial intelligence.

Republia carried out research to define vulnerabilities of the industry and consider vulnerabilities, which would be eradicated by Republia Ecosystem.

The data collected were analysed , based on information obtained from various resources of submitted projects, as well as official documents, websites, forums etc.

CRITERIA FOR COMPARATIVE ANALYSIS

- **Hardfork** - is a change in the source code, which entails mandatory update of nodes of the network and, eventually, separating from core network

- **SCAM projects** - in the blockchain industry emergence of scam projects means the emergence of companies, which for various reasons ceased to fulfill its obligations to investors.

- **Smart contract vulnerabilities** - are possible errors and violations that are detected during the execution of smart contract.

- **Network throughput** - is maximum number of transactions that can be processed by the network during a certain period of time.

- **Data theft** - is the loss of important, confidential user data after networks or programs are hacked, which entails loss of information and funds.

- **Impact of individual users on the network** - the process, where participants influence on the network unequally and where some individual users, according to different criteria, get a priority right to make decisions.

- **Master nodes and nodes that perpetrated a fraud** - users(master node or node) deceive other users when carrying out their responsibilities in the network.

- **Transition of a smart contract to an infinite loop** - the process when smart contract is not executed due to errors in the code, which causes transition of a smart contract to an infinite loop. So this contract will be executed during unlimited period of time and network overload will occur because of constant use of network resources.

RESULTS

Comparative analysis is based on a comparative study of popular projects, which provide the industry with technologies, implemented using blockchain of its own design. The data below have been compiled on the basis of information from articles, websites, videos and other materials, available in public domain.

Results based on many aspects for comparison

Table 1.1

Probability-based criterion	Republia	Nem	Bitcoin	ICON (ETH TOKEN)	NEO
Hardforks	Impossible	High	High	Middle	High
Emergence of scam projects	Very low	High	High	High	High
Smart contract vulnerabilities	Very low	High	No smart contracts	High	High
Network throughput	High	low	Very low	low	low
Data theft	Very low	Middle	No ecosystem	Middle **	Middle
Impact of individual users on the network	Impossible (RepubliaID)	Above	High	Above the average	Above the average
Master nodes and nodes that perpetrated a fraud	Impossible (ZEROing)	Middle **	Middle	Very low (Casper) **	Middle
Transition of a smart contract to an infinite loop	Impossible	Impossible	No smart contracts	Impossible	Impossible

Results based on many aspects for comparison

Table 1.2

Probability-based criterion	Republia	EOS*	Tezos*	Ethereum	Waves
Hardforks	Impossible	High*	Impossible*	High	High
Emergence of scam projects	Very low	High*	High*	High	High
Smart contract vulnerabilities	Very low	Above the average*	Very low*	High	Middle
Network throughput	High	High*	low*	low	Middle*
Data theft	Very low	Very low*	Middle*	Middle	Middle
Impact of individual users on the network	Impossible (RepubliaID)	Above the average*	Above the average*	Above the average	High
Master nodes and nodes that perpetrated a fraud	Impossible (ZEROing)	Middle*	High*	Very low (Casper)*	Middle
Transition of a smart contract to an infinite loop	Impossible	Impossible*	Impossible*	Impossible	Impossible

Legend of network throughput
(volume of transactions in the network per 1 second)

High	More than 40'000
Middle	From 5'000 to 40'000
Low	From 1'000 to 5'000
Very low	Less 1000

* Characteristics that were not verified in mainnet

** Data were entered at a rough estimate because of the lack of information.

COMPRASION

Decentralized Republia ecosystem, through its voting system which leads to decision-making by consensus, and then, automated update of the protocol among users, solves the problem of both hardforks and scam-ICO, because users decide independently whether they want to see a project within the ecosystem.

In Republia ecosystem all users are provided with equal opportunities and can equally influence the development of the network through the unique Republia ID, which, in turn, is implemented into the voting system. Thus, it guarantees that one user can vote only once within one voting.

Republia also offers triple-layered security - Veracity System, all important information is stored in CloudX, which prevents theft of user data.

Rebublia Blockchain consists of multiple chains and solves the problem of low network throughput due to dynamically increasing number of sidechains.

Since Republia protocol is implemented using functional programming language OCaml, which, while supporting formal code verification, minimizes hacking of smart contract code. In the Republia Smart Contract Platform smart contracts will not go to an infinite loop, because Republia Virtual Machine operates under a timestamp principle.

The fraud, which is perpetrated by master nodes and nodes, is solved by introducing "ZERO.ing" tool (freezing a certain number of RPB for the subsequent participation in recording of blocks and receiving rewards). In the case of fraud, this amount is charged from the account of the malicious user, so network members will not have intention to harm the ecosystem when their personal funds are at risk.

NEM

The throughput of NEM network is only 120 transactions per minute and it operates using POI algorithm (Proof Of Importance), which means unequal influence of users on the network, since the significance of a particular participant depends on the proof of storing certain amount of funds and the number of his transactions.

Therefore, more significant user will be able to initiate a hardfork without the consent of a majority of participants.

BITCOIN

Bitcoin network is known for the number of hardforks. Only during the period from 2017 to 2018, there were 30 hardforks.

In addition, Bitcoin has the lowest network throughput among all submitted projects (7 transactions per second). Also, in the Bitcoin network the main role is performed by pools. 27% of all the capacities involved in the network belongs to BTC.com, which is the largest pool . While a simple user is not allowed to have even the slightest impact on the modernization of Bitcoin network.

ICON

ICON project is an open source ecosystem, its goal is to unite projects based on the blockchains of other networks.

Thus, there is a high probability of the emergence of scam projects on the basis of ICON network, since various organizations and projects can join it without any limitation of their number and ideology.

NEO

The main disadvantage of NEO network is centralization , since its blockchain system is private. Moreover, the network throughput is only 1000 transactions per second.

Since blockchain of this network is private, individual users have an impact on the network. As for vulnerabilities of NEO smart contracts, at the end of May 2018 the developers found errors in the code of smart contracts that are used by cryptocurrency tokens of NEP-5 standard .

EOS

Only 21 participants will have an impact on EOS network, who will be chosen by the community, according to DPoS algorithm. Such a restriction can lead to the seizure of the network by a group of people, who will make changes that are not agreed by other participants.

TEZOS

Tezos is based on Proof of Stake algorithm, which means that one user has a large volume of assets . Thus, it is possible that a group of people will possess sufficient supply of assets to have a full-scale impact on the network.

ETHEREUM

Majority of ICO campaigns are launched by Ethereum Platform , as this platform promotes various projects, as shown by huge number of tokens (80,000 of tokens as at May 1, 2018), as well as by the number of investors who were deceived.

Tokens of ERC-20 standard are, in fact, smart contracts, which have received general acceptance for proven efficiency. However, many people do not take into account their risks, for example, since a smart contract can not be changed after it is created, it may contain errors and vulnerabilities that will lead to a loss of funds.

Hacking of DAO in 2016 led to the split of the Ethereum network and the creation of Ethereum Classic.

The problem of DAO is that EVM code is implemented using statically typed programming language called Solidity, that is similar to JavaScript.

WAVES

WAVES platform provides an opportunity to place any ICO project, without restrictions. Thus, the platform is being expanded by competitive ICO, which increases the risk of emergence of Scam projects in the industry.

The platform operates on the basis of LPoS consensus, which means that only full nodes affect the network. Other users can only transfer earned balance to them for lease and can not participate in mining.