Proceedings of the SMART–2018, IEEE Conference ID: 44078
2018 International Conference on System Modeling & Advancement in Research Trends, 23rd–24th November, 2018
College of Computing Sciences & Information Technology, Teerthanker Mahaveer University, Moradabad, India

Blockchain and Smart Contracts for Support the Interaction between the Actors in the Regional Innovation System

Alexey Finogeev[1], Sergey Vasin[2], Leyla Gamidullaeva[3] and Danila Parygin[4]
[1,2]*Professor, Penza State University, Penza, Russia*
[3]*Associate Professor, Penza State University, Penza, Russia*
[4]*Associate Professor, Volgograd State Technical University, Volgograd, Russia*
E-mail: [1]alexeyfinogeev@gmail.com, [2]pspu-met@mail.ru, [3]gamidullaeva@gmail.com, [4]dparygin@gmail.com

***Abstract*—The paper covers the issues of development of a mechanism for ensuring reliable and secure interaction among participants in regional innovation systems based on the establishment of smart contracts in the blockchain. The technology allows to reduce the possibility of fraud by dishonest participants, as well as to exclude the need for a third party by transferring its functions to a smart contract. This mechanism is important for ensuring confidential and transparent relations between participants in innovative projects, as well as with all interested stakeholders in regional economic system.**

Keywords: Interaction Management, Cyber-Social System, Multi-Agent Approach, Benchmarking, Big Data, Intellectual Analysis, Region

I. Introduction

The strengthening of interactions between interested participants in a regional system appears to be an important mechanism of innovation activity development from the emergence of an idea to the commercialization of innovation. As a rule, there are growing instability and uncertainty of existing links and relationships at innovation activity stages, which, in particular, stimulate the growth of transaction costs. This determines high costs of development and implementation of innovations. Such costs are not of transformational nature associated with transformations and changes of initial resources, but of transactional one that is determined by a necessity of collaborations and mutually beneficial contacts. Therefore, one should consider transaction costs as a barrier to the innovative development in the regions demotivating companies when implementing innovations [1,2].

It is reasonable to use cyber-social technologies to organize and support an innovation system that simplify and promote interactions between innovation activity participants by performing a situational analysis of large arrays of structured and unstructured data on innovation activity subjects in the regions. An innovation system that actively uses the said technologies when interacting with many other regional innovation activity participants will ensure the synergetic effect. Such IS is an adaptive intelligent information system uniting social and intellectual processes [4]. It may be implemented in the form of an Internet-portal linking regional innovation medium participants (innovation infrastructure facilities; universities and research centers; small, medium and large companies; state bodies and structures; users and the community).

II. Blockchain and Smart Contracts for Support the Interaction of Innovation Stakeholders

It should be noted that elements of any cyber-social system depend on the provided safe and reliable interaction within transaction processes aimed at elaboration and implementation of development mechanisms, including the innovation ones. The trending transition to digital economy means that the most processes of informational interaction should be carried out with minimal human involvement. At the same time an important role in digital economy is assigned to safety and transparency of transactions between interacting agents that should be provided by blockchain and smart contracts.

It is known that purchasing, selling and renting various products and services on the Internet and by online commerce is a complicated task. The main problem is trust relationships or a lack thereof between unacquainted transaction participants. To solve this problem it is required to address the third party for guarantees of transaction settlement. But even in this case the problem of safety is not resolved by high reliability. In risk management the technology of the distributed register (blockchain) is being applied more actively, as it reduces the probability of fraud from dishonest participants and excludes the need for the third party by transferring its functions to the intelligent system [5].

Blockchain is a specifically structured uninterrupted sequential chain of blocks (chained list, distributed register) containing information on participants and existing innovations [6]. Copies of blockchains are stored

and processed independently from each other in multiple network nodes [7,8]. Originally the term referred to the completely replicated distributed data base (register) designed for the "Bitcoin" system, as the technology was initially intended for cryptocurrency transactions. Although blockchain can be applied to any interconnected information objects. All data are stored in network nodes of users of the distributed register system. Each node stores a part of information in the form of data blocks or copies of such blocks. This principle makes the system virtually invincible to information threats and attacks, all the more these blocks are protected by cryptographic keys and calculated using the algorithm of hash-functions. The advantages of blockchain are transaction transparency and multiple copying of transactions so that each participant always has information about the steps taken by all partners. It is important for ensuring trustful and transparent relationships between innovation project participants, as well as other interested regional subjects of the socioeconomic activity. The blockchain technology offers the distributed storage to save data required to complete a transaction or any informational interaction of many participants (agents). The technology is capable of storing the following data: product or service documentation, financial transaction records, contractual obligations, personal data, intellectual property rights, copyrights, digital description of intellectual property entities, company information, etc. One of the advantages of the technology for innovation systems is a possibility to lodge authorship without the third party or any geographical binding. The authenticity of informational objects is proved by a digital certificate. By virtue of blockchain authors can prove copyrights and intellectual property rights. The technology ensures safe storage of updated information on any innovation objects.

The distributed register will make it possible to track the life span of innovation activity results and the impact of these results when creating innovations. For example, open-access scientific publications are sources for patent creation. Researchers who publish such results often are university employees uninvolved in economic processes. At the same time, patent holders may use published results of somebody's research when registering intellectual property rights without referring to these results. If we build a blockchain of intellectual property objects and scientific publications, than the register will help track down the process of sharing and using knowledge when synthesizing new results of the intellectual activity. It will be possible to identify the author of an idea and to distribute remuneration. For example, Ascribe company by means of blockchain helps artists prove authorship rights to pieces of art using unique identifiers and digital certificates. The procedure of ownership rights transfer from artists or authors to buyers or collectors is also provided for [10].

The objects of smart contracts may be the following:

- Interacting parties accepting or declining contract's conditions via digital signatures,
- Contract's subjects including objects in the field of contract's existence,
- Conditions that display a logic of contract clause execution in the form of a formalized mathematical description, which can be programmed in the field of contract's existence.

In turn, the existence of smart contracts requires as follows:

- Application of digital signatures on the basis of public and private keys through asymmetric encryption,
- Presence of open distributed data bases for storing of data on executable transactions with access for contracting parties,
- Availability of a distributed network to execute Ethereum, Codius, Counterparty contracts, etc.,
- Digital data source validation, for example, by means of SSL certification centers.

Today modern blockchain platforms are used to develop decentralized applications (DApps). Although decentralizaed applications are similar to smart contracts, they have no direct connection with funds and enable to utilize blockchain for any means [14]. DApps have no limitations in the number of participants and they are independent from market segments.

III. Blockchain Platforms for Smart Contracts and Dapps

Among modern blockchain platforms one should distinguish Ethereum, Aeternity, Hyperledger Fabric, Cardano [15].

The Ethereum platform and the cryptocurrency of the same name are intended for creation of smart contracts and DApps [16]. The platform enables to create DApps and use the Internet for transactions of any complexity. It is designed as a uniform decentralized virtual machine. Based on the given platform the smart contract technology allows to register any transactions with assets in the distributed base of contracts realized through hashing in blockhains. Ethereum users ensure calculation of hash totals by themselves in their computers. The Ethereum system runs on the embedded programming language-Solidity, using which one can write new smart contracts with random ownership parameters, transaction formats and status changing functions.

The Aeternity platform offers a unique solution to the scaling problem, so that smart contracts have no effect on the said parameter [18]. The system functions on the basis of the Lightning Network payment protocol [19], which operates with blockchains and executes instant transactions between nodes settling the problem of scaling. It adds the logical level assuming the load of an increasing number of

transactions. At the same time, the transactions between participants within smart contracts take place in dedicated channels without including the whole blockchain into the process. The main blockchain is used only as the distributed register to make account of financial consequences of successful transactions or as a decentralized arbitrator in case of controversies.

The Hyperledger Fabric platform is the open blockchain for universal application [20]. The project was launched in 2016 supported by IBM and JP Morgan. The platform is capable of synthesizing applications and utilizes the technology of blockchain multilayer configuration. The last version features private transaction channels distinguished by high reliability and throughput.

The Cardano platform is a blockchain platform of the third generation [21]. The system is designed to provide scalable programmed transfer of cryptocurrency value. The blockchain is written in Haskell programming language. The main distinctive feature is the division of computing layers. In particular, the system has a settlement layer for the ADA cryptocurrency turnover and a layer to handle smart contract synthesis and operation. The system applies a consensus algorithm on the basis of Proof-of-stake, in which the probability of creation of a block in the chain by a participant is proportional to his/her share in cryptocurrency units. This makes it possible for owners to control transactions in the network, to increase power efficiency and scalability.

In the course of the research the Ethereum blockchain platform was selected to create smart contracts during safe and reliable information interactions between subjects of a regional innovation system. The Ethereum system includes the following tools: Geth, Parity, CPP-Ethereum, Solidity, Remix, Truffle, Webpack, Web3.js, etc.

The system issues smart contracts as decentralized applications written on an object-oriented JavaScript-like language-Solidity. The contracts are compiled in the Remix cloud development environment enabling to write and launch the code directly in a browser. Following the transition into bytecode they are executed by the Ethereum virtual machine realized on network computing nodes.

Proof-of-Work is applied to build a consensus mechanism on the Ethereum platform. It confirms the transaction authenticity by network's computing power, and the probability of the next block creation depends on this power. At the present time Ethereum is being transferred to the Proof-of-Stake algorithm, which would eliminate this dependence.

Such programs as Geth, Parity, CPP-Ethereum are designed to link nodes to blockchain. They are downloaded to computers as clients and run the Ethereum protocol. It is possible to work with blockchain through web-sites using special browsers or add-ins like MetaMask and Mist. The latter are a connecting link between popular browsers and blockchain enabling to perform tasks and send commands to blockchain.

Browsers and blockchain may also interact through the Web3.js library that helps working with Ethereum nodes via

Remote Procedure Call (RPC) through HTTP, launching JSON files written in JavaScript as shown in figure 1.

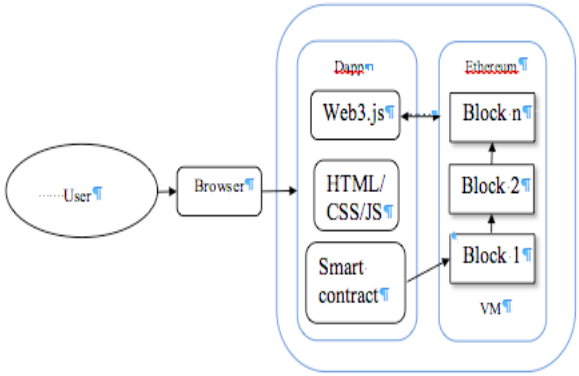

Fig. 1: Working with a Decentralized Application and Blockchain Via a Browser

IV. Results and Conclusion

To create a blockchain system of interactions between subjects of regional innovation system it is necessary to choose a platform and to develop a series of components on its basis that execute various transactions. The system must provide safe and reliable conclusion of contracts and accomplishment of contract obligations when developing and implementing innovations, as well as transfer of intellectual property rights, carrying out the stipulations of license agreements, transparency, protection and conservation of data on innovations and innovation companies, opportunities for rights and licenses usage monitoring in the course of innovation activities, etc. One of the system's components is a distributed register of transactions with digital copies of innovation objects that basically represents a chronological digital notarial system. It keeps record of such transactions as innovation object registration, granting access to a digital passport of an innovation object, results of expert's examination of an innovation object, object assessment by various criteria, object registration in a ledger, description of an object ownership right transfer, mutual financial settlements, author's remuneration payment, settling disputes on intellectual property rights, etc.

The next system's component is smart contracts. They offer a chance to complete multiple tasks occurring in the course of interaction between innovation system's participants, in particular:

To create digital innovation assets and cryptocurrency for mutual settlements;

To collect funds for implementation of innovations (crowdfunding);

To identify users;
To confirm authenticity of files and documents;
To confirm and check intellectual property rights;
To adopt systems of digital voting and data accounting;
To create decentralized innovation asset exchanges, etc.

An agreement for concrete IAR is created using a client web-application. The information about the agreement is entered into blockchain as a smart contract. Such contract is impossible to deceive, therefore, IAR ownership can be transferred only by the entity specified as «Current owner» of the contract. To fix IAR in a blockchain the owner pays a fee. As soon as IAR have been fixed in the blockchain, it is allocated a unique identifier by a computed hash total, visualized in the form of a QR-code on the web-site together with the information on innovations available for exchange or sale, as shown in figure 3. A potential buyer can acquire IAR using a browser or an installed mobile app. The mobile app scans a QR-code and then sends a user to the site with detailed information on IAR, including the following: IAR's author, all previous IAR's owners, date of IAR acquisition and registration, information on a patent (certificate of registration), IAR description, etc. Ownership transfer launches a function assigning the next potential owner. When the owner acknowledges IAR, the system confirms new owner's property rights. The information about the new owner is added to the smart contract, thus synthesizing a block with new hash total. The described operation is paid for by the buyer (Fig. 2).

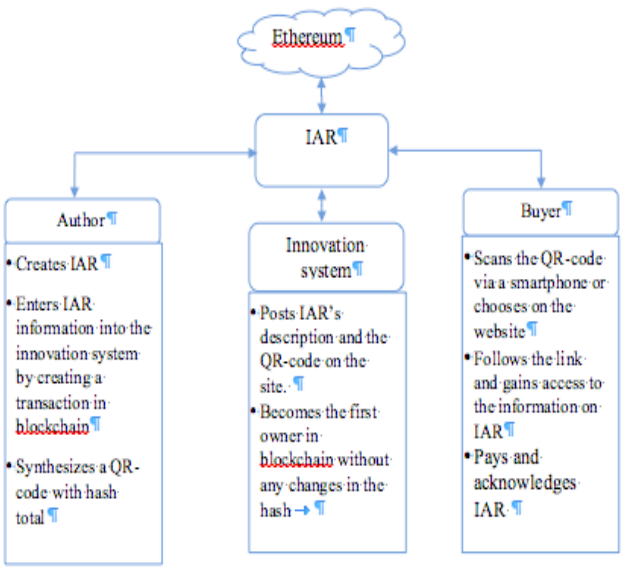

Fig. 2: A Scheme of Smart Contract Functioning for IAR

Initially, to create the blockchain system there were installed such tools as Node.js v6 + LTS, Git, Ganache, VisualStudio Code, the Truffle framework and the web3. js library. A lite-server was deployed for web-applications functioning. Smart contracts are developed and adjusted online via IDE Remix allowing to compile and tune contracts, as shown in figure 3.

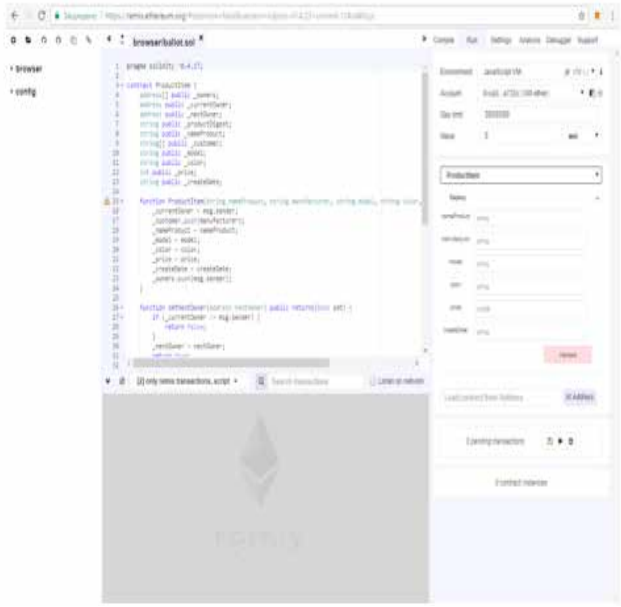

Fig. 3: Remix Integrated Development Environment

For a smart contract to be launched in blockchain it is necessary to install the Ethereum client–Ganache, as well as the Metamask add-in to work in a browser.

The main part of the system's business logic when interacting with innovation activity subjects within smart contracts is that users' actions are fixed in blockchain, as shown in a UML use case diagram (figure 4).

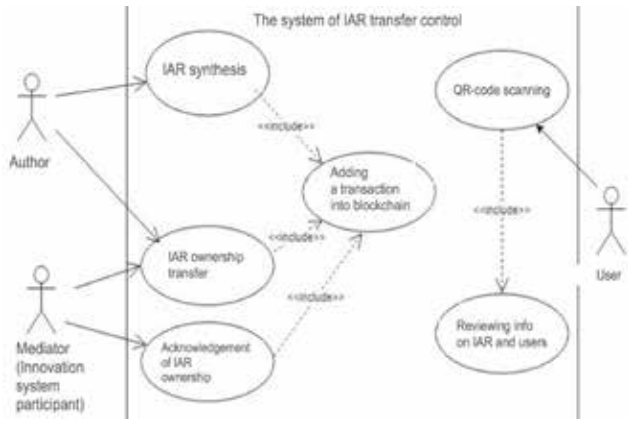

Fig. 4: UML Use Case Diagram

The paper considers issues of creation of a new mechanism providing reliable and safe interaction of regional innovation system's participants on the basis of smart contracts created in blockchain.

Further on it is planned to create smart contracts to accomplish various operations, transporting services for convenient exchange of information on transactions, an innovation monitoring and control system for state authorities, etc.

The implementation of smart contract tools into regional management of innovations will make it possible to connect innovation producers and users, to ensure safety

and transparency of their operations, to accumulate the experience of joint innovation projects, to reduce transaction costs for participants and potential investors.

Acknowledgement

The reported study was funded by Russian Foundation for Basic Research (RFBR) according to the research projects № 18-010-00204, № 16-07-00031, № 18-07-00975.

References

[1] Vasin, S.M. and Gamidullaeva, L.A., (2015), 'Development a Basic Model of the Innovation System,' Review of European Studies, 7(11). [Online], http://dx.doi.org/10.5539/res.v7n11p175

[2] Gamidullaeva, L.A., Chernetsov, M.V., Vasin, S.M., Taktarova, S.V. Enhancing economic growth through innovation in Russia: Identifying key incentives for innovation Proceedings of the 30th International Business Information Management Association Conference (IBIMA) 8-9 November 2017 Madrid Spain. Vision 2020: Sustainable Economic development, Innovation Management, and Global Growth. P. 2684-2697.

[3] Gamidullaeva, L.A., Tolstykh, T.O. Transaction Costs, Institutions and Regional Innovation Development: the Case of Russia. Proceedings of the 30th International Business Information Management Association Conference (IBIMA) 8-9 November 2017 Madrid Spain. Vision 2020: Sustainable Economic development, Innovation Management, and Global Growth. P. 2121-2135.

[4] Finogeev, A.G. 2004. Simulation of systems-synergistic processes in information environments. Penza: Penza State University, p. 223.

[5] Blockchain in Russia. 2018. http://www.tadviser.ru/index.php/Статья:Блокчейн_в_России#cite_note-7 Retrieved on 17 June 2018.

[6] Swan, M. 2015. Blockchain: Blueprint for a New Economy.— O'Reilly Media, Inc., p. 152.

[7] Franco, P. 2014. The Blockchain. Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons, p. 288.

[8] Antonopoulos, A. 2014. The Blockchain. Mastering Bitcoin. — O'Reilly Media, Inc.

[9] In Russia may appear a blocking analogue of eBay in the field of intellectual property management. https://forklog.com/v-rossii-mozhet-poyavitsya-blokchejn-analog-ebay-v-sfere-upravleniya-intellektualnymi-pravami/. Retrieved on 17 June 2018.

[10] Official site of Ascribe company. https://www.ascribe.io/

[11] In Russia may appear a blocking analogue of eBay in the field of intellectual property management. https://forklog.com/v-rossii-mozhet-poyavitsya-blokchejn-analog-ebay-v-sfere-upravleniya-intellektualnymi-pravami/ Retrieved on 7 June 2018.

[12] Szabo, N. 1997. Smart Contracts: Formalizing and Securing Relationships on Public Networks. First Monday. 2, 9. http://firstmonday.org/ojs/index.php/fm/article/view/548/469

[13] Smart Contracts, Explained. Partnership Material, https://cointelegraph.com/explained/smart-contracts-explained

[14] Decentralized platforms for smart contracts: challenges and solutions. https://forklog.com/detsentralizovannye-platformy-dlya-smart-kontraktov-vyzovy-i-resheniya/

[15] Blockchain platforms. http://smart-contracts.ru/platforms.html

[16] Blockchain app platform. https://www.ethereum.org/

[17] Solidity is a contract-oriented, high-level language for implementing smart contracts. http://solidity.readthedocs.io/en/v0.4.24/

[18] Aeternity blockchain. https://aeternity.com/

[19] Poon, J., Dryja, T. 2016. The Bitcoin Lightning Network: scalable off-chain instant payments. http://lightning.network/lightning-network-paper.pdf

[20] Hyperledger Fabric is a platform for distributed ledger solutions. http://hyperledger-fabric.readthedocs.io/en/release-1.1/

[21] Cardano is a decentralised public blockchain and cryptocurrency project and is fully open source. https://www.cardano.org/en/home/