

New way of transfer of ownership on intellectual property objects of Avionic based on Blockchain technology.

Offered to Intellectchain platform based on Blockchain for control, store and transfer ownership intellectual property objects [1]. Intellectchain designed to accelerate and facilitate the introduction of scientific research, development, discovery into real industrial use.

Analysis of current trends of blockchain technologies and practical implementations of these technologies in projects allows us to note the following basic concepts and achievements:

Blockchain is a growing list of records, called blocks, which are linked using cryptography [2][3]. Each block contains a cryptographic hash of the previous block [3], a timestamp, and transaction data (generally represented as a Merkle tree root hash). The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta [3][4]. They wanted to implement a system where documents' timestamps could not be tampered with or backdated. In 1992, Bayer, Haber and Stornetta incorporated Merkle trees to the design, which improved its efficiency by allowing several documents to be collected into one block [3][5]. The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. It was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network [2].

Smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible [6]. Smart contracts were first proposed by Nick Szabo in 1994.

Ricardian contract is a contract in which all conditions defined on language understandable for human and machine. As invented by Ian Grigg in 1996 [7].

Byzantine fault tolerance (BFT) in cryptography it is the task of interaction of several remote subscribers who received decree from one center. Some subscribers, including the center, may be intruders. It is necessary to work out a unified strategy that will be beneficial for subscribers. Leslie Lamport proved that in a system with m malfunctioning processes (malefactors), it is possible to reach agreement only if there are $2m + 1$ true process, that is, strictly more than two thirds of the total number of processes [8].

Smart law is a smart contract that contains conditions and limitations of the state legislation.

The application of blockchain in the state and society in the near future will make it possible in principle to simplify and improve transparency, the degree of trust

between the participants in such processes as electronic voting, the transfer of ownership of material and intellectual objects, registration of birth certificates, changes in marital status, issuance of documents, certificates, etc.

Blockchain introduction problems: one of the significant problems of implementing blockchain technology in the life of society, in addition to the human factor, is the low throughput of transactions and high requirements for the amount of stored data on each node (each node stores all the transactions inside the system). A solution to this problem can be a mechanism for cutting off the head of transaction histories, from most of the nodes involved in processing current transactions, and archiving these data in separate audit nodes. In this case, each node has the actual current state of the system without a huge archive of old transactions, which allows all nodes to use less resources for the further operation of the entire system and provide greater throughput. Audit nodes are used only to resolve disputes (where throughput requirements are significantly lower).

Etherium is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality [9]. It supports a modified version of Nakamoto consensus via transaction-based state transitions. Ether is a cryptocurrency whose blockchain is generated by the Ethereum platform. Ether can be transferred between accounts and used to compensate participant mining nodes for computations performed [10]. Ethereum provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network [9] [11]. Ethereum was proposed in late 2013 by Vitaliy Buterin, a cryptocurrency researcher and programmer. The system went live on 30 July 2015.

Microsoft Azure Blockchain Workbench is a cloud platform for simple and rapid design, construction and implementation of blockchain projects on the basis of smart contracts. Supports the following platforms of smart contracts: Corda (R3 company), Ethereum, Hyper Ledger Fabric (Linux Foundation). In particular, this platform provides and facilitates the interaction between smart contracts concluded on various platforms.

Offered to Intellectchain platform based on Blockchain for control, store and transfer ownership intellectual property objects [1]. Intellectchain designed to accelerate and facilitate the introduction of scientific research, development, discovery into real industrial use. Main participants Intellectchain: author, company, expert.

Standard use case of Intellectchain:

- The author, as a result of research and scientific work has produced an intellectual product that can be useful for the industrial industry.
- Author preparing three kind of detailing of own intellectual product:
 - Annotation – for public domain.
 - Expanded describe - for expert checking.
 - Full describe – for make a deal.
- The author signs all three documents with his unique key (author token) and places the annotation of his intellectual product in the intellectchain system and classifies it (or the system helps him to classify it) within the sectors and

industries. The abstract is kept in the public domain and any interested person can get acquainted with it. Also, in the system stores hashes of an extended and full description, but not the documents themselves.

- Company from matched Industry, receives information about new intellectual object acquainted with it and, in case of interest, informs about intention get expanded describe and also expert review. Company signs this intention with its unique key (company token).
- Expert, from matched subject area, receives notification about new intellectual object which need in review. Expert signs their readiness to review with its unique key (expert token).
- If author trusts the expert (based on history and ratings) he signs permission to check of intellectual object for this expert (using author token) and provide access to expanded describe of this object. Intellectchain don't store expanded describes, system just check accordance of transferred document to originally expanded description (by hash). Also, the system registers the fact that the expert has access to an extended description.
- Expert is check intellectual object and leave and signs review.
- Based on expanded description and expert review - company decides (or not) that this intellectual object is interesting for them. And enters into negotiations with the author, regarding the conditions of provided full describe of intellectual object and transfer intellectual property rights.
- In the event that the company and the author have reached an agreement, the terms of this agreement are signed by a unique key of the author and the company, after which the author provides access to the full description of the product (in the case of the executed terms of the transaction). The company fulfills the conditions (makes payment or any other conditions) and automatically receives a full description of the intellectual product (indicating the list of transferred rights).
- All conditions and intentions and facts of the transfer of documents, their authenticity (originally signed by the author's documents) are registered in the system as transactions (smart contracts).
- If an unscrupulous expert or company or author violates the terms of a smart contract, the contract is automatically canceled.
- Risks:
 - Unscrupulous expert when he got acquainted with the extended description - assigns this part of the intellectual object to himself and tries to get from it an economic benefit outside the intellectchain system.
 - The company, having concluded and having executed the smart contract with the author for acquaintance with the full description of intellectual product, but not having concluded the contract on transfer of the rights of possession by this intellectual product, after acquaintance starts to use an intellectual product of the author without informing him about it.

- The author originally prepared scam for the third complete specification of his intellectual product, and the company, having fulfilled the terms of the contract, receives a virtually random document.
- Intellectchain provides only confirmation and guarantee that the initially signed documents are used in smart contracts by the author, but it does not know what is actually stored in them (except for the annotation).
- All these controversial situations can lead to some participants of executed smart contracts have received a scam. In this case, each participant must seek justice in court, the intellectchain system can only confirm the transfer of documents and values between the participants and the conditions of these smart contracts were concluded. In the United States, there is already a precedent for the recognition and consideration of a smart contract by a court.
- All participants of the system make a decision on their trust to each other, of course taking into account the ratings of the history, rating of authors, their projects, experts, and companies.
- To reduce the mistrust factor, it is possible to split the description into more than three levels, and to establish the conditions for obtaining access to each description by the author himself, for an ever-increasing reward with ever increasing trust of the author to the company, the company to the author and his intellectual product.

First variant Intellectchain based on [1] realized on site www.intellectchain.com which passes alpha-testing and optimization. Proposed classification of intellectual objects based on classification of NYSE American [12], next development involves the use of Microsoft Azure Blockchain Workbench platform.

References

1. Zemlyansky V.M., Zakrevskiy O.O., Gusev M.O. Method of control, storage, movement and transfer of intellectual property rights. Application for invention a **2018 08144** in UKRPATENT, filing date 23 July 2018
2. Parkins, David "Blockchains: The great chain of being sure about things". *The Economist*. 31 October 2015.
3. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.
4. Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". *Journal of Cryptology*. 3 (2): 99–111.
5. Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992). *Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences*. 2. pp. 329–334.

6. Tar, Andrew "Smart Contracts, Explained". Cointelegraph. 31 October 2017.
7. I. Grigg. The Ricardian Contract. In Proceedings of the First IEEE International Workshop on Electronic Contracting, pages 25-31. IEEE, 2004.
8. Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem". ACM Transactions on Programming Languages and Systems. 4 (3): 382–401.
9. Understanding Ethereum (Report). CoinDesk. 24 June 2016.
10. Chohan, Usman W., MBA, Cryptocurrencies: A Brief Thematic Review 4.08.2017.
11. ConsenSys (23 June 2016). "Ethereum, Gas, Fuel, & Fees"
12. finviz.com