Decentralization of the issue-based knowledge transfer platform

© Vitaliy Tsyganok[0000-0002-0821-4877], © Mykyta Savchenko[0000-0003-1107-0461],
© Sergii Kadenko[0000-0001-7191-5636] and © Oleh Andriichuk[0000-0003-2569-2026]

Institute for Information Recording of National Academy of Sciences of Ukraine, Kyiv, Ukraine

tsyganok@ipri.kiev.ua, zitros.lab@gmail.com,
seriga2009@gmail.com, andriichuk@ipri.kiev.ua

Abstract. We consider issue-based computer platforms, designed to transfer knowledge in a way, that ensures its thorough and effective utilization in various domains. Such platforms have subsystems for collecting knowledge and for decision-making support. Typically, these systems are centrally located and store data in one specific place, such as a data center, or even in one database, where this data can be easily lost or damaged. In addition, this data can be spoofed or altered anonymously in many ways, if traditional software or hardware access to it is attacked or misused. These problems can be partially solved by introduction of proper security and monitoring solutions, using the best security practices, such as secure protocols and first-class encryption. However, this article offers methods that, practically, eliminate the very possibility of data falsification, and add other important properties to computer systems, such as data invariability, decentralization, and fault tolerance of the data registry or individual subsystems of issue-based knowledge transfer platform.

Keywords: knowledge transfer platform, expert knowledge collection system, issue-based computer systems, decision support system, decentralization, blockchain.

Introduction

There is a global dilemma of the most thorough use of available knowledge. The effectiveness of applying this knowledge to various subject domains is one of the most important factors contributing to overall human progress. According to the research, conducted by a US company Delphi Group at the beginning of the current millennium [1], a significant share of knowledge (more than 40%), used by a certain organization is non-formalized and not even registered in any kind of data storage. This knowledge is based only on the skills, experience, and intuition of certain experts.

There is no doubt that when making decisions in different fields of activity, it is necessary to rely on all available knowledge, both stored somewhere and provided by an expert ad hoc. This is especially true for loosely structured data, characterized by high level of uncertainty and incompleteness.

The first stage of solving of the above-mentioned problem could be integration of knowledge of different formats, obtained from different time-dependent sources, with formalized knowledge and knowledge that experts provide. If combined with processing and storage of this formalized data in databases, this approach can become an ultimate solution. Each next transfer of accumulated relevant knowledge for its further use in decision-making process can be the final stage of decision-making, which brings the desired results. An example of the implementation of this approach is the issue-based hardware and software platform of knowledge transfer, created according to the chart, shown outlined on Figure 1.

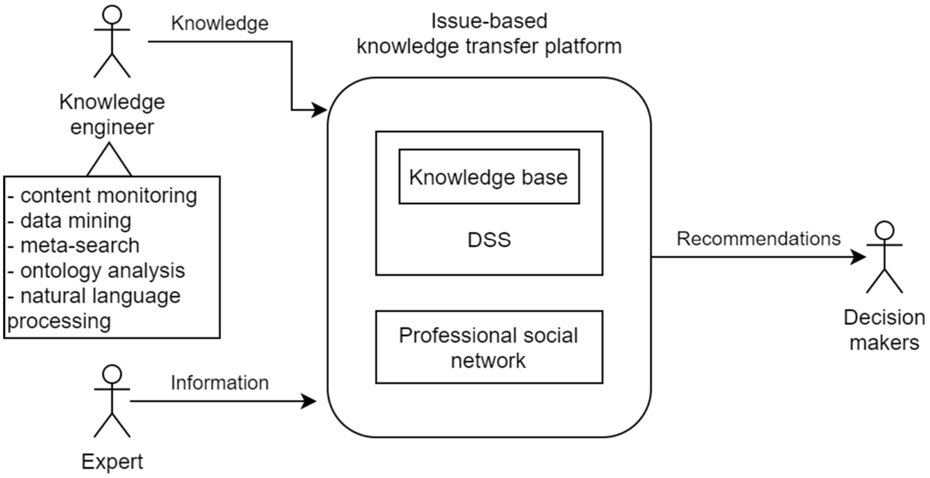

Fig. 1. Issue-based platform of knowledge transfer: a chart

Functionally, the knowledge transfer platform is represented by the following components:

1. The subsystem of knowledge collection and actualization, which is designed to support the experts' workflow, knowledge engineers (expert session organizers) and decision-makers (DMs). The main functions of this subsystem are:

- user registration and accounting.
- assessment of competence for engineers and experts, which provides insights on what knowledge fields they are most experienced in [3].
- building of a knowledge base, containing a model of subject areas (performed by knowledge engineers). This also includes conducting an expertise (expert session).

2. The subsystem for providing knowledge and decision support system (DSS) itself are intended for:

- choosing the best solution for DMs.
- evaluation of decisions in uncertain conditions.
- strategic planning.
- generating and predicting future scenarios, etc.

It is assumed that the knowledge engineer, who is also the main actor in the system and who has knowledge in specific subject domains, is using these tools for automated extraction of knowledge and for organizing expert sessions. Engineers, using DSS tools, create models of subject domains and knowledge databases. Later, based on these models and knowledge, decision makers get recommendations from the system. Functionally, in the knowledge transfer platform, the decision support system (DSS) is responsible for generating recommendations [2, 3]. Another component of the platform is a professional social network, which unites specialists-experts in various areas of study, and utilizes them as another source of knowledge. This social network also measures the relative competence of each expert, which is considered during decision support process. Later, the measured competence is also used to determine the financial reward for each expert [4, 5].

1 On the necessity of knowledge transfer platform decentralization

In this paper, decentralization means the use of a cryptographically protected decentralized data platform, which works based on blockchain technology. Decentralizing a centralized system is an important process, which can also be considered a mandatory one, if there is a need to ensure timely and ultimate data protection against unauthorized interference and targeted attacks. Before blockchain was invented, this task was solved using multiple secure layers and geo-decentralization, which, however, could not guarantee absolute data protection.

System decentralization process is the transition of the system from fully centralized to partially or fully decentralized mode. Decentralization makes sense if we need the system to assume the following properties [6]:

- Guarantee of data storage in the immutable, global distributed data registry. This registry cannot store large amounts of data, but neither it is necessary for the purpose of data protection [7].
- The impossibility of forgery (modification) of stored data in a way that was not foreseen in advance, including the impossibility of incorrect insertion, processing, and deletion of data from this registry. The most vulnerable part is the decentralized program which manages the data, but not the data itself. The decentralized program must be properly written, audited, tested and stored. These steps ensure, that decentralized programs will function only in the prescribed manner, programmed once and forever [8]. It is also worth noting that there are other types of attacks, such as, for

instance, a theoretical threat of hacking blockchain platform after adoption of quantum computers, since the latter have much higher computational performance than traditional computers and can break the underlying blockchain algorithm. However, modern decentralized data platforms, based on blockchain technology, have already implemented algorithms to make blockchains quantum-resistant. So, probably, attacks of this kind will not be successful [9].
- Execution of previously defined set of calculations only (on the blockchain level).

When it comes to decentralization of systems built with decentralized data platforms, the following types of decentralization should be outlined:

- **Full decentralization**. Systems of this type assume that their computational part, including the data management and storage subsystems, is also decentralized and, therefore, cryptographically protected. This is only possible when the program is fully stored in a decentralized data platform, and no parts of the system are outside that platform. Modern decentralized data platforms, such as Ethereum and similar ones, allow you to create the so-called decentralized programs that are loaded into a decentralized data registry only once and can never be changed again. This immutability gives strong security advantages, but it means that the software should foresee all possible scenarios of interacting with it in advance, because, after being loaded, it will never ever be changed. Thus, there will be no practical possibility of data forgery and any other methods of interference with the originally uploaded program. This also requires the program to be carefully reviewed for any vulnerabilities before uploading it to the decentralized registry [10].
- **Partial decentralization**. As of 2021, there is no decentralized data platform that can scale indefinitely. All of available data platforms have their own limitations: mainly bandwidth (the number of transactions per unit of time is limited) and the presence of fees for using the platform. These problems are usually solved through partial decentralization, since full decentralization of the system is either too expensive or impractical.
- **No decentralization**. All traditional computer and software systems, i.e. systems that do not use decentralized data platforms, are centralized. Centralization in the context of software systems means that there are one or more institutions that can at least somehow affect the operation of the system, control it and/or its data. It should be noted that system security and its decentralization are different concepts; secure systems in the classical sense are still centralized.

The level of decentralization of any system is determined not only by how it uses decentralized data platforms and integrates with it, but also by decentralization level of the decentralized data platform itself (for instance, which algorithm it uses to protect data and computation centralization). However, this problem is out of scope of this article [11].

When it comes to distributed systems for collecting expert knowledge, which can be related to partially decentralized systems, the knowledge transfer platform acquires the following important properties:

- Guaranteed reliability of expert knowledge storage, including permanent availability of this storage for a small (but sufficient) amount of data needed for DSS system, and complete protection against unauthorized changes. This property is especially important for expert systems and knowledge-based systems, because often the results of a certain examination, after its completion, must be stored for a long time, for example, up to 10 years from the moment of completion of some research projects.
- Possibility of conducting a public audit of the system later, based on reliable input data, stored in the decentralized registry. Since the data, stored in the decentralized registry, is cryptographically protected, there is no doubt in its authenticity. Using this reliable data, assuming that the DSS is idempotent when performing calculations (it produces the same result with the same input data), it is possible to verify the result and the reliability of the source data by performing the calculation again.
- As a result, we have increased confidence in the functioning of the knowledge transfer platform, which also increases the credibility of results, obtained from the DSS.

An alternative to decentralization of the subsystem for collecting expert knowledge of an issue-based knowledge platform is the use of electronic digital signatures (EDS) and several centralized data registers (like traditional databases). It is worth noting that even in the case when these alternatives are used, the knowledge collection system still won't have the properties, listed above [12].

2 The model of knowledge transfer platform using the full decentralization

A recently conducted research demonstrates, that in a typical system of expert knowledge collection, the total amount of data (which primarily consists of expert estimates) recorded in the decentralized register is small, and occupies less than 500 kilobytes of storage space per project. Since the results obtained and stored by the DSS may be in demand (reviewed and used) for quite a long time after the project completion (in extreme cases, up to 10 years), we conclude, that for such systems it makes sense to store all input information in a decentralized register. In other words, a complete decentralization of a system, which collects expert knowledge, means partial decentralization of the knowledge transfer platform itself, since the system of expert knowledge collection is its subsystem.

However, full decentralization of a system always makes it somewhat difficult for the user to work with it. After decentralization it is necessary to have not only a decentralized account (also known as a "wallet" in cryptographic decentralized data platforms), but also a certain number of cryptocurrencies to pay for transactions in the decentralized network. This problem is classified as a problem of adoption of technology and is one of the reasons why many systems and products cannot integrate with decentralized technologies just yet [13]. However, with the help of the originally developed transaction delegation method [14], this interaction is simplified to only creating an account in the decentralized data platform, without losing any properties of a fully decentralized system.

After decentralization, the system, which collects expert knowledge, will not have fundamental differences from the previous version of the system, except for several additional prerequisites the experts should do before working with the system. There are also a few steps, which knowledge engineers should also do, but only once before starting any project:

- Creating a decentralized program which will be uploaded to the decentralized data platform. This program can be templated, that is, developed once, and only slightly modified for each specific subject domain using pre-programmed parameters.
- Creating a delegate account and providing it with the cryptocurrency, necessary for further decentralized transactions which experts will perform.
- Experts, in turn, do several additional simple steps: before entering their estimates into the system, each expert generates his(her) own decentralized account, and uses the graphical user interface to register it in a decentralized program (separately for each expert session project or only once, depending on the system design), thereby authenticating in the system, and confirming his(her) identity. Experts can associate any additional data with this identity. No one but experts themselves can input evaluations on their behalf after such registration in a decentralized system.

Figure 2 shows a sequence diagram, describing the steps, required for work with the decentralized system (from the administrator of the knowledge transfer platform / knowledge engineer) and the procedure of performing a delegated transaction on behalf of an expert.

The preparation work consists of the following steps:

1. The administrator develops (or clones an existing) decentralized program created for a specific expert system (or uses a template). The function of this program is to perform a cryptographically protected entry of the expert data into a decentralized register with the help of a delegate, for further reading by the decision support system.
2. The administrator registers this program in a decentralized data platform, thereby making it immutable. It obtains a unique application address, which is also immutable.
3. The received address of the decentralized program is written into the centralized storage (or program code) of the expert system for further interaction with it.

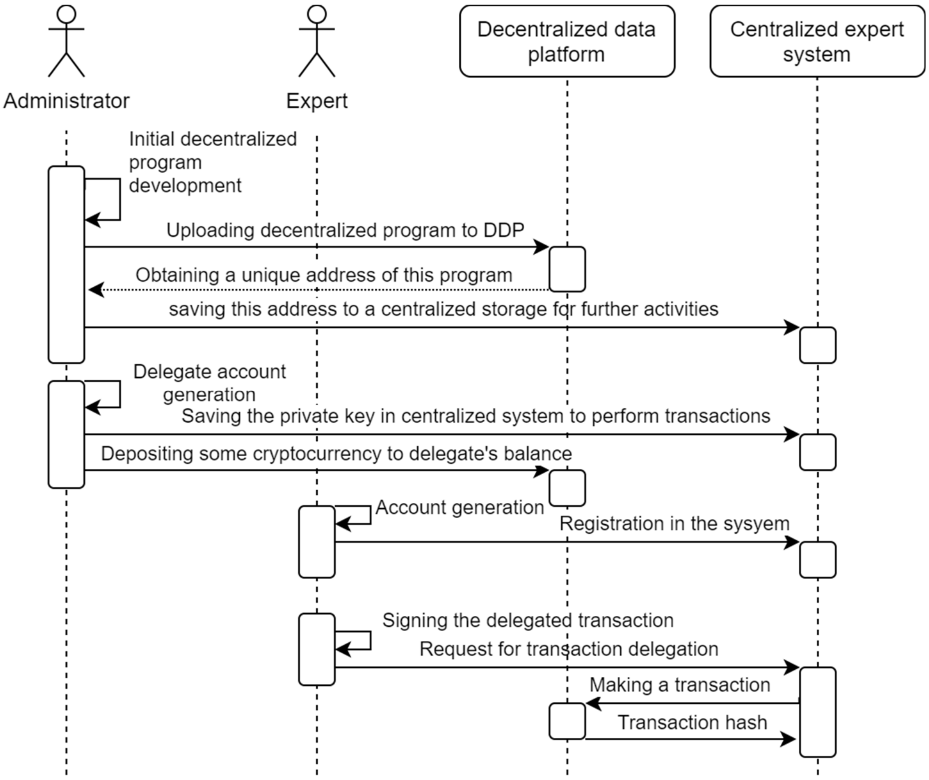
Administrator
Expert
Decentralized data platform
Centralized expert system
Initial decentralized program development
Uploading decentralized program to DDP
Obtaining a unique address of this program
saving this address to a centralized storage for further activities
Delegate account generation
Saving the private key in centralized system to perform transactions
Depositing some cryptocurrency to delegate's balance
Account generation
Registration in the sysyem
Signing the delegated transaction
Request for transaction delegation
Making a transaction
Transaction hash

Fig. 2. Prerequisites required for a decentralized system and implementation of delegated transactions

4. Additionally, the administrator generates a delegate account and replenishes its balance in a decentralized system. The delegate account is also stored in the delegated transaction support system, which can a be part of the decision support system.
5. Before starting to work with the system, experts create their decentralized accounts (for example, using the browser extension called Metamask) and register them in the centralized system by creating electronic digital signatures for certain pieces of data, requested by the system (for example, an email address). Thus, they confirm that they are the owners of this decentralized account.
6. After the work with the system is done, the expert performs a delegated transaction to write the generated data into the decentralized storage. This transaction is genuine, and no one but the expert himself can change this data after it is stored in the decentralized registry, and, moreover, at any time anyone can check the correctness of the data, that was written into the decentralized network (although this is not necessary).

While expert knowledge is processed by the decision support system, the data is read from a decentralized registry and converted into a format, that is convenient for processing. In future, data from the decentralized registry can also be used, for example, to audit a certain expertise (session). Figure 3 shows the interaction of an expert and the centralized expert data collection system with the decentralized program before and after the examination (i. e., how experts work and read data from a decentralized register).

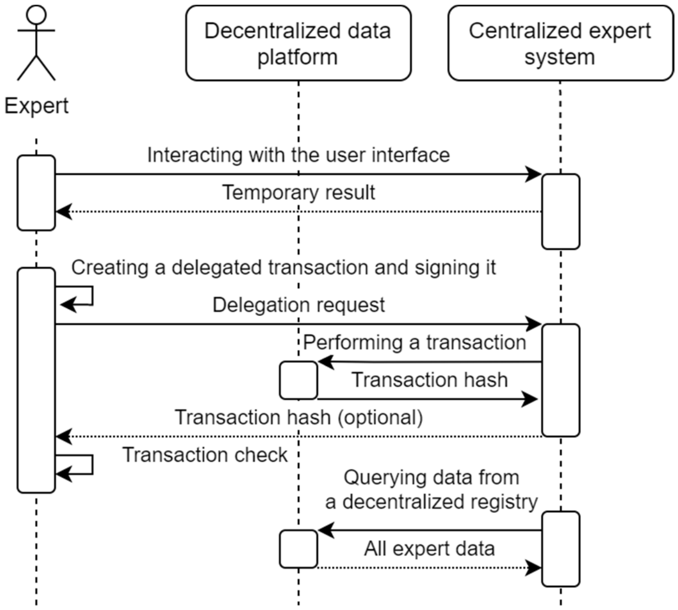
Expert
Decentralized data platform
Centralized expert system
Interacting with the user interface
Temporary result
Creating a delegated transaction and signing it
Delegation request
Performing a transaction
Transaction hash
Transaction hash (optional)
Transaction check
Querying data from a decentralized registry
All expert data

Fig. 3. The system collecting expert data using a decentralized data platform

3 Results of decentralization of the expert knowledge collection system

After decentralization, when the changes, suggested in the paper, were applied, the (previously centralized) system of expert knowledge collection, acquired the following properties:

1. The input data, obtained from experts, is now protected and maintained by a global decentralized data platform, which guarantees its storage and immutability.
2. Since the data is cryptographically secure and immutable, it is considered a reliable source of credible knowledge (provided that the decentralized program is correct, which can be easily verified at any time). This allows us to increase the level of trust to the decision support system itself, and to conduct a post factum auditing of the system, if necessary.

In order to implement the above-listed properties within the system, only minor changes had to be introduced into the existing centralized system.

Here they are:

1. The need for experts to install an additional (relatively simple) software, as either a mobile application or a browser plugin. This approach, in its turn, can also completely replace the process of registration in the expert data collection system using traditional login and a password.
2. Adding two new steps for the expert to perform: electronic data signature before (registration) and after (executing a data recording transaction in a decentralized register) working with the centralized system.

Conclusions

The result of the conducted research is the method proposal for decentralization of the issue-based knowledge transfer platforms, which include subsystems for knowledge collection and decision-making support. The proposed improvements can significantly increase the security of information storage and processing in the system, allowing it to prevent any loss, as well as unauthorized storage-level changes of information and changes to the original software.

As a result of decentralization, the data, obtained from experts, is protected and maintained by a global decentralized data platform, which guarantees its lifetime storage and inability of intruders to compromise it. Once recorded, cryptographically protected data remains unchanged and can be considered a reliable source of information, also verifying that if the centralized software is correct and unchanged. The suggested approach completely eliminates the possibility of data falsification and adds important properties to the system, such as invariability and fault tolerance. As a result, decentralization allows to increase the level of confidence in the knowledge transfer platform and perform open system audits when necessary.

Acknowledgement

This work has been produced in collaboration with the European Union's Horizon 2020 research and innovation programme under the grant agreement N 830943, ECHO project.

References

1. Tuzovskiy A.F., Chirikov S.V., Yampolsky V.Z. Systems management of knowledge (methods and technologists). Tomsk : Yzd-vn NTL, 2005. 260 p.
2. Tsyganok V.V., Borokhvostov I.V., Roik P.D. Problem-oriented knowledge transfer platform for decision making support in socio-technical systems. *CEUR Workshop Proceedings,* Vol. 2067 Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017); Kyiv, Ukraine, November 30, 2017. P.112-117.

3. Tsyganok V., Kadenko S., Andriichuk O., Roik P. Combinatorial Method for Aggregation of Incomplete Group Judgments. *Proceedings of 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*. Igor Sikorsky Kyiv Polytechnic Institute. Kyiv, Ukraine. 08-12 October, 2018. P. 25–30.
4. Totsenko, V.G., Tsyganok, V.V. Method of paired comparisons using feedback with expert. *Journal of Automation and Information Sciences*. 1999. 31(7-9). P. 86–96.
5. Tsyganok, V.V., Kadenko, S.V. On sufficiency of the consistency level of group ordinal estimates. *Journal of Automation and Information Sciences*. 2010. 42(8). P. 42–47.
6. Savchenko M., Tsyganok V., Andriichuk O. A Cost-Effective Approach to Securing Systems through Partial Decentralization. *Information & Security: An International Journal.* 2020. 47, no. 1. P. 109-121.
7. Shafagh, H., Burkhalter, L., Hithnawi, A. and Duquennoy, S., 2017, November. Towards blockchain-based auditable storage and sharing of iot data. *In Proceedings of the 2017 on Cloud Computing Security Workshop.* (pp. 45-50).
8. Moubarak, J., Filiol, E. and Chamoun, M. On blockchain security and relevant attacks. *In 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)* April, 2018. P. 1-6.
9. Fernández-Caramès, T.M. and Fraga-Lamas, P., Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, 2020. 8. P. 21091-21116.
10. Skichko D., Grinenko T. O., Narezhna O. P. Security of blockchain technology for decentralized systems. *Global Cyber Security Forum* : *materials of the First International Scientific and Practical Forum*, November 14 – 16, 2019. Kharkiv : NGURE, 2019. – P. 98–99.
11. Gochhayat, S.P., Shetty, S., Mukkamala, R., Foytik, P., Kamhoua, G.A. and Njilla, L. Measuring Decentrality in Blockchain Based Systems. *IEEE Access*, 2020. 8. P. 178372–178390.
12. Savchenko M., Tsyganok V., Andriichuk O. Decision Support Systems' Security Model Based on Decentralized Data Platforms. *CEUR Workshop Proceedings*, Vol. 2318 *Selected Papers of the XVIII International Scientific and Practical Conference on Information Technologies and Security (ITS 2018)*. Kyiv, Ukraine, November 27, 2018. P.209-221.
13. Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H. and Weber, M. On the financing benefits of supply chain transparency and blockchain adoption. *Management Science*. 2020.
14. Savchenko M., Tsyganok V., Andriichuk O. An Approach to Transaction Delegation in Self-protected Decentralized Data Platforms. *CEUR Workshop Proceedings*, Vol. 2577 *Selected Papers of the XIX International Scientific and Practical Conference on Information Technologies and Security (ITS 2019)*. Kyiv, Ukraine, November 28, 2019. P.169-188.