A Conceptual Model for Blockchain-Based Software Project Information Sharing

Musa Erhan[1], Ayca Tarhan[2][0000-0003-1466-9605], Adnan Ozsoy[2][0000-0002-0302-3721]

[1]TUBITAK BILGEM ILTAREN, Ankara, TURKEY
musaerhan06@gmail.com
[2]Hacettepe University, Department of Computer Engineering, Ankara, TURKEY
{atarhan, adnan.ozsoy}@hacettepe.edu.tr

Abstract. Accurate estimations play a significant role in the success of software projects, and companies should have sufficient number of past project data to make these estimations accurate and reliable. Some institutions gather project metrics from companies to create cross-company datasets and open these datasets to companies for paid or free of charge. On the other hand, many companies do not want to make public all or part of their project information so it prevents the growth of such datasets. Blockchain technology and smart contracts, as a medium to store private information and share it with predefined constraints, might be a solution to this problem. In this study, we propose a conceptual model as a reference for blockchain-based software project information sharing, and discuss issues related to its feasibility.

Keywords: Blockchain, Software Project, Information Sharing, Access Control, Conceptual Model

1 Introduction

Companies need past project data to establish software estimation practices and improve software project planning and management processes. A company can create its own within-company dataset from past projects. However, there are problems when relying on a within-company dataset [1]: (i) the company needs time to collect enough data on past projects; (ii) even if it has collected enough data in time, the company might have made changes on data for new projects, which could make their previous measurements not usable; and (iii) all data should be collected and kept consistently.

These problems have motivated the use of cross-company datasets. A cross-company dataset is a collection of project data that are collected voluntarily from several companies [2]. Some institutions aim to provide cross-company datasets by collecting project information from software companies either as part of a membership or for free. In case of membership, the company providing data can have access to the entire project database. Free access, similarly, allows all users to access project data gathered so far. However, this kind of access mechanism does not consider privacy issues neither on

project nor attribute basis. As a result, companies that do not want to share all or part of their project information avoid data entry to these datasets.

In this work, with an aim to support creation of larger and trustable cross-company datasets, a conceptual model for blockchain-based software project information sharing is proposed. The conceptual model gives the owner of project information the authorization to determine access controls on the basis of project attributes. Basic features of blockchain technology such as data distribution, access-permission, and immutability have been considered in identifying operating principles underlying the conceptual model. For example, a company may add project information to the system with all attributes being accessible to third-parties, selected attributes being accessible to third-parties and others being private, or all attributes being private only for its own access. Accordingly, this company is assumed to make estimations more accurately based on its own project attributes at least, and based on other companies' project attributes as allowed for sharing by their owners in larger contexts. By this kind of access control mechanism, companies that do not use existing datasets for privacy reasons are expected to participate with the proposed model. It is also expected that the model will motivate the creation of larger cross-company datasets on which effective project estimations will be realized.

The remaining of this work is organized as follows: Section 2 provides background on several known software project datasets and the basics of blockchain technology, together with a summary of related work that shed light to the creation of the conceptual model. Section 3 explains the conceptual model and its elements, demonstrates its operation over an example scenario, and discusses the feasibility of the proposal. Section 4 concludes the paper with highlights from this initial study and plans for future work.

2 Background and Related Work

2.1 Software Project Datasets

According to the study [3], Desharnais, ISBSG, and COCOMO datasets are widely used for software project estimations. Below are brief descriptions of these and another widely used QSM database.

- Desharnais [4][5]: The most commonly used publicly available dataset in the field of software effort estimation. It consists of 81 projects collected by J.M. Desharnais.
- ISBSG [6]: There are different subscription options to access ISBSG dataset. It includes data for more than 9,000 IT projects.
- COCOMO [7][8]: COCOMO'81 is another publicly available dataset. It includes data 63 projects.
- QSM Software Project Database [9]: The QSM database has over 13,000 completed software project metrics. Access to QSM database is done through QSM SLIM Tools [10][11] provided by the owner of the dataset. To avoid identification of data owners, access to data can only be done in summary form which is the result of provided tools.

Although these datasets and some others have been subjected to numerous software project estimation studies in both literature and industry, they have some common drawbacks in storing and sharing data in general, as we list below:

- They do not consider different roles with respect to data (e.g., owner, verifier, and user) in storing and sharing of project information.
- There is no attribute-based access control mechanism for storing and sharing project information. Although all project information in many software project datasets (e.g. in ISBSG) is anonymized before it is added to the pool in order to prevent traceability of data owners, we cannot say that this is a decentralized access control mechanism because once the data is added to the dataset, the central authority has full control of the data. In QSM dataset, on the other hand, access to the dataset is provided through tools to secure the data, and the complete control of the data is not in the data owner but in the dataset owner.
- The number of project entries is limited (except ISBSG and QSM datasets) because of the lack of access control mechanism mentioned above. Nevertheless, it is expected that project entries to ISBSG and QSM datasets will increase with the attribute-based access control mechanism that can only be managed by the data owner.
- In most cases, the previously shared project information cannot be withdrawn or closed to access in time.
- Once shared, the datasets are managed by third-party users and therefore, the reliability of data is restricted to the reliability of these users.
- On the basis of reliability mentioned above, there is no mechanism to prevent project information being tampered or hacked by an external user.
- There is no well-defined incentive mechanism to motivate project owners to share their project information.

The issues mentioned above highlight the need for a role-based, access-permissioned, and trustable infrastructure for software project information storage and sharing. We propose by this work that blockchain technology and smart contracts, as a medium to store private information and share it with predefined constraints, might be a solution to this need. In the following section, we highlight the basics of this technology as the base for our proposal.

2.2 Blockchain Basics

Blockchain [12] is a distributed database that provides encrypted transaction tracking. It is invented by Satoshi Nakamoto whose real identity is still unknown. In blockchain, each record is digitally signed and a combination of records form so called ‘block’. Each block contains the previous block’s hash value, making a connected chain of blocks. This connected structure in blockchain avoids any alteration in the records, thus making it immutable. Its distributed nature gets rid of the need for a central authority for processing any transactions. So, the operations can be carried out directly between the buyer and the seller safely. Blockchain is a way for users to agree on something even if they do not trust each other. Fig. 1 [13] shows how blockchain works.

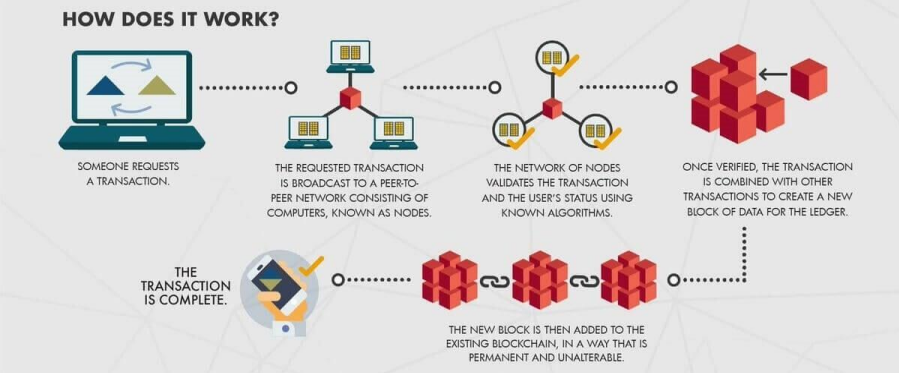

Fig. 1. A Look at Blockchain Technology [10]

Below is the list of main features of a blockchain:

- *Immutability*: Once a block added on the chain, it cannot be altered. So, it prevents corruption.
- *Decentralization*: A copy of the current information in the blockchain network is stored in different nodes. Blockchain does not need a trusted authority. Since there is no trusted authority, there is no one with ultimate rights to change the blockchain data for their own benefit. So only users who own the data can manage their data.
- *Security*: Blockchain security is based on cryptographic features such as asymmetric encryption and hash functions.
- *Transparency*: The history of the records can be followed by everyone.

There exist two major types of blockchain technology which are public and private. In addition to the main features that are mentioned above, both types have different features. Below is the list of the benefits of public blockchains:

- *Open Read/Write*: Anyone can submit transactions to the blockchain and can view all data related to transactions.
- *Distributed Ledger*: Each node is equal so the blockchain is immutable and censorship free.
- *Secure*: Anyone can be a node and contribute to the security of the system. With a lot of nodes in the network, it is much harder to attack the system.

The benefits of private blockchains are:

- *Faster Transactions*: Private blockchain nodes distribute locally. This makes the performance faster.
- *Scalability*: Main scalability issues are related to consensus algorithms. But there are a number of fast consensus algorithms especially for private blockchains.
- *Member Control*: Only approved participants can submit transactions, and non-approved users cannot access to the blockchain. Therefore, no extra operations like encryption is required to prevent unauthorized users from accessing data.

- *Energy Consumption*: There are many consensus mechanisms with private blockchains that achieve consensus by consuming less resources.

Bitcoin [12] is the first and most popular digital currency that uses public blockchain technology. Sending bitcoin operations takes place in the peer-to-peer network. It is faster especially compared to the SWIFT international money transfer system. Since there is no central authority, it is not under the control of any institution, organization or person. Bitcoins are created using the processing power in the distributed network that is called mining.

Later in 2015, Vitalik Buterin proposed Ethereum [14] that is a public blockchain-based computing platform. It enables the development of decentralized software protocols using its own special language. It has a cryptocurrency called Ether. Ether production is carried out by Ethereum miners. While cryptocurrency transfer was the main operation within the Bitcoin network, Ethereum aims to be a distributed computing environment in which users could integrate software applications on blockchain along with making cryptocurrency transfer. Ethereum Virtual Machine [14] is the infrastructure that runs programs called smart contracts on the Ethereum. Smart Contracts [14] are programs that can run automatically on the blockchain and work to meet certain conditions. Smart contracts are lines of code that are stored on blockchain. When set of defined rules are met, smart contract automatically runs and produces results.

Hyperledger [15] is a Linux Foundation open source project that provides a variety of projects for building private blockchain networks for business. It primarily focuses on creating distributed ledger for institutions and business networks. For this purpose, different systems and tools have been developed in order to adapt to changing needs. Hyperledger is definitely not a cryptocurrency like Bitcoin and Ethereum. Smart contracts can be defined to execute logic that generates new facts that are added to the ledger like Ethereum.

Tokens represent an asset or benefit on project ecosystem. Owners can use tokens to access a service. The cryptocurrencies such as Bitcoin and Ether are tokens, but every token does not have to be a cryptocurrency. Some tokens are designed to be used within the market created by the application in which they are related.

2.3 Related Work

Blockchain data sharing with privacy has been studied by a number of researchers in recent years. We provide an overview of their related works below.

Azaria et al. [16] proposed a system called Medrec to handle medical record management using blockchain technology in 2016. With this system they aim to manage authentication, confidentiality, accountability and data sharing for, sensitive medical information. They use Ethereum and smart contracts to log patient information.

In 2016, Cruz et al. [17] proposed an authentication mechanism system suitable for the trans-organizational utilization of roles. Their system makes role-based access control using Bitcoin protocol. They designed a challenge-response authentication protocol to verify ownerships of roles.

Xia et al. [18] proposed another system MeDShare that provides medical data sharing in cloud repositories. The system uses smart contracts and access control mechanism for all actions on data. They claim that sharing medical data with research and medical institutions with data privacy can be ensured by this system.

In 2018, Cruz et al. [19] proposed a role-based access control mechanism using Ethereum and smart contracts. Their mechanism verifies a user who owns a role by using a challenge-response authentication protocol. They compared their mechanism with other mechanisms based on smart contacts and Bitcoin blockchain.

In 2018, Desai et al. [20] proposed a data sharing agreement protocol which uses blockchain. Their protocol creates smart contracts based on agreement protocol and shares data in exchange for payment. Their framework includes a voting mechanism that can impose penalties. Their framework can be used for different kinds of terms associated with data sharing agreement.

In 2018, Ozyilmaz et al. [21] proposed a blockchain-based Internet of Things data marketplace using Ethereum and smart contracts. They used Swarm [22] as the distributed storage platform. They aimed to make IoT device vendors and Artificial Intelligence and Machine Learning solution-providers work together.

In 2019, Kabi et al. [23] proposed a physical goods marketplace application using Ethereum. Their application enables trading of goods without a third-party. They measured the performance of the system based on gas which is a unit for computing power to execute an operation in Ethereum Virtual Machine.

3 Blockchain-Based Conceptual Model

To investigate the feasibility of a role-based, access-permissioned, and trustable infrastructure for software project information sharing, a blockchain-based conceptual model has been developed. In this section, we explain details of the model, demonstrate its operation over an example scenario, and discuss its likely limitations.

The proposed model has an attribute-based access control mechanism for sharing project information. In this way, a company can manage access controls on the basis of project attributes and share all or part of its project information. The company can also manage previously shared project information and its access controls. In addition, an incentive mechanism is proposed to motivate project owners to add project information to the system. Since the proposed model is blockchain-based, its execution does not require a managing authority. In this way, all transactions to be performed on the data are under the authority of the data owner and the sharing of data cannot be tampered or censored without the consent of the project owner. In addition, thanks to the immutable feature provided by blockchain technology, the stored project information does not carry the risk of being modified by hacking attacks.

3.1 Requirements and Assumptions

Blockchain-based conceptual model has three roles as data provider, verifier, and data user. The model offers several benefits to these roles. The data provider gains tokens in

exchange of project information. Verifier, who will be selected among data providers having similar project information, earns tokens to verify the added project information. By motivating data providers to add project information, it is assumed that a large amount of project information will be added to the system and the reliability of these data will be ensured by the verification operations. The data user will have access to a large amount of reliable data generated by this model and in return he/she will pay token for the project information used.

Access control of project information is enabled through project attributes. In this way, the data provider can share a certain part of its project information and keep the other parts private. Data provider grants access for the project information via project attributes. In this regard, blockchain technology provides significant benefits for the proposed model. Since blockchain has decentralized feature and there is no central authority, the access and management controls of the project information can be performed only by data provider. This enables the data provider to trust the system. Since the data is stored in the blockchain in a distributed manner, there is no risk of losing data. The immutable feature of blockchain ensures that the project information saved in the chain will not be tampered without the consent of the owner.

3.2 Conceptual Model

Fig. 2 shows the graphical representation of the blockchain-based conceptual model. We explain the concepts and their relations following the figure.

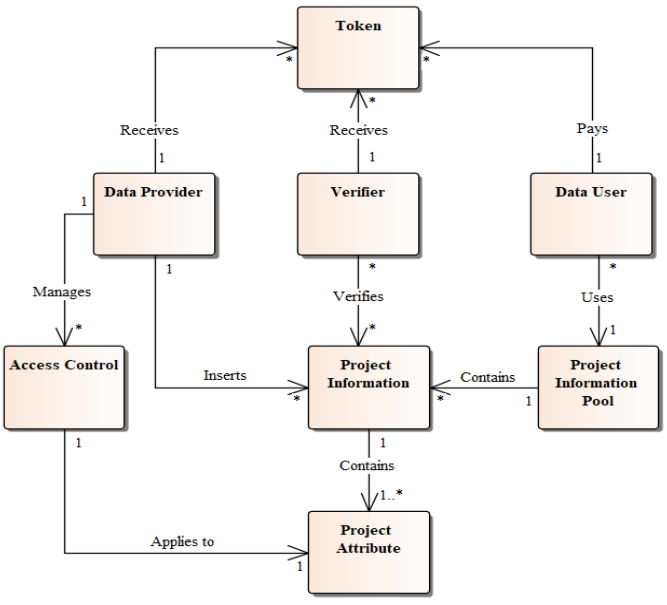

Fig. 2. Conceptual Model for Blockchain-based Software Project Information Sharing

Data Provider: The data provider can insert project information to project information pool and manages access controls of already inserted project information. Access controls are managed by associating data users (or user groups to be defined) with project attributes that the data provider wants to grant access to. By this way, project information sharing is enabled per allowed attribute. Only the data provider owning project information is authorized to manage access controls. The data provider receives tokens in return for project information used by the data user. If the data provider does not give access right to anyone, he/she cannot earn tokens. Yet the data provider can access and use his/her own private project information.

Verifier: When the data provider adds project information, a number of data providers who have similar project attributes are assigned as verifiers. Similarity decision can be made by using project attributes like project type such as embedded system and project size measures such as functional size. Verifiers are selected from data providers who have been granted access to project information. Therefore, the verification cannot be done if the data provider does not give access to any other data provider. The reliability rating of inserted project information is determined according to the verification results. The value of rating which is verified by more verifiers will be higher. This value indicates the reliability of project information for data users. The verifier wins tokens after completing the verification process.

Data User: The data user makes queries in project information pool and uses project information that is granted access by data providers. Access to project information will be allowed on the project attribute basis. The data user pays tokens in exchange for using project information. The data user can evaluate the reliability of a project information according to its rating value. The project information which has higher rating value is more reliable because it is verified by more verifiers.

Project Information Pool: The project information pool is a collection of all projects' information. The information that data providers have added and data users have used is located in this repository. These data can be used in carrying out software project estimations by project managers.

Project Information: The project information defines the data of a software project. It contains project attributes of a software project.

Project Attribute: A project attribute is a piece of information that determines the properties of a software project. For example, a project attribute can be defined as type of software project which can be embedded system or mobile application. Access control of a project information is made on the basis of project attributes. In this way, a data provider can make a part of project information accessible and another part of project information private.

Access Control: Access control mechanism is used to enable data providers to add project information with the authorization restriction that they want. All access control management operations can be done by the data provider who is the owner of project information.

Token: The tokens are used to motivate data providers, verifiers and data users. It enables all roles to benefit from the system. The data provider is motivated to add project information. The verifier gains tokens by verifying project information. The data user will be able to access more reliable project information. It provides a win-win situation for all participating roles.

3.3 Example Scenario

Based on the conceptual model explained in the previous section, Fig. 3 demonstrates the main flow of operations in sharing, verifying and using project information via the blockchain-based infrastructure. Numbers in the figure shows the order of operations in the flow.

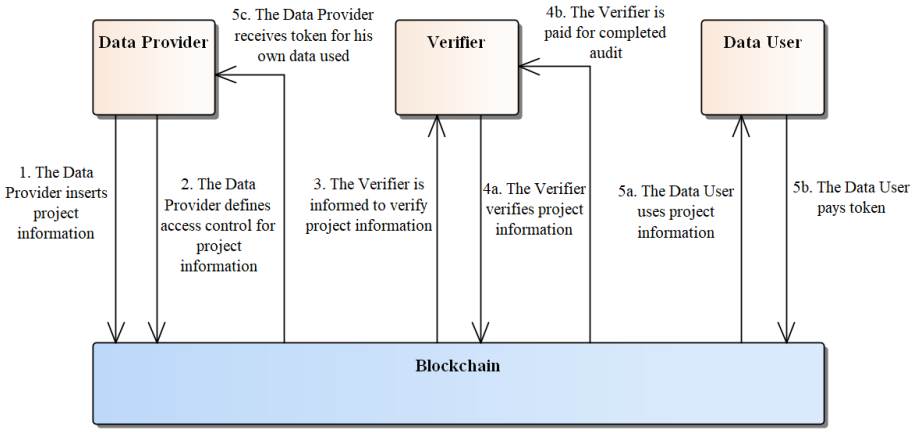

Fig. 3. Main Flow of Operations in Sharing and Using Project Information

The following operations are executed in sequence in the main flow of the example scenario:

1. The data provider creates project information and its project attributes. Then he/she inserts created project information into project information pool.
2. The data provider grants access rights for the project information via project attributes.
3. The verification request is made to inform the verifiers.

4. a. The verifier checks whether project information is proper and verifies it. Verification result determines the value of the project information rating.
   b. The verifier receives tokens when the verification process is completed.

5. a. The data user queries project information pool with respect to certain criteria to obtain the project information data set that he/she want to use. Project information that the data user has access rights is displayed.
   b. The data user pays tokens for using project information.
   c. Token payment is made to the owners of project information used by the data user.

The scenario described above can be realized by developing a software application that will use the underlying blockchain technology. Smart contracts can be implemented for the data store and access control mechanism. The use-case diagram of such a software application to carry out the operations in the scenario is given in Fig. 4 with respect to three roles defined as the actors.

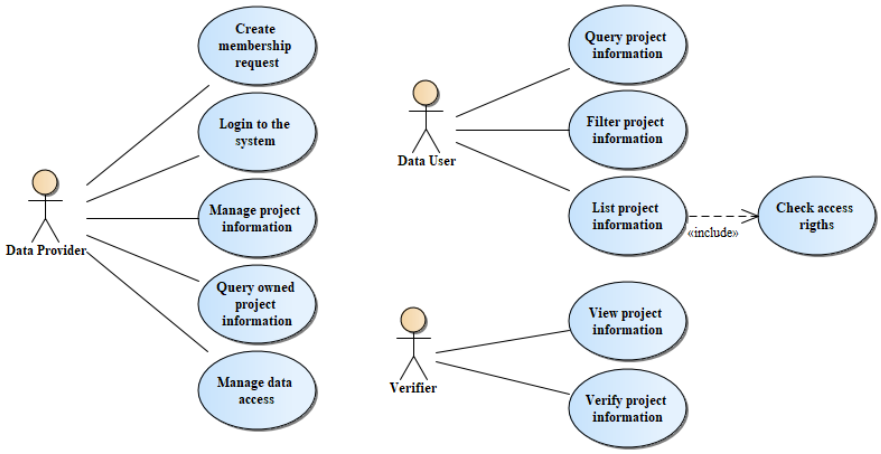

Fig. 4. Use Case Diagram for Realizing the Example Scenario

The proposed conceptual model is designed to store and share project information in different data sets. In order to illustrate the use of the model, the following mapping table is given in Table 1. In the table, a sample part of ISBSG dataset in Fig. 5 is adapted to the conceptual model.

Table 1. Concepts and ISBSG Dataset Mapping

Proposed Concept	ISBSG dataset
Project Attribute	A Cell (Ex: Manufacturing)
Project Information	A Row (Ex: Project information with ID 10132)
Project Information Pool	All Rows
Data User	Customer of Dataset
Verifier	Dataset Repository Manager
Data Provider	Data Owner of a Row
Token	None. Only paid membership for Data Users
Access Control	Centralized, repository-based

	Rating	*Rating*	*Software Age*	*Major Grouping*	*Major Grouping*	*Major Grouping*
ISBSG Project ID	Data Quality Rating	UFP rating	Year of Project	Industry Sector	Organisation Type	Application Group
10132	B	B	2010	Manufacturing	Manufacturing;	Business Application
10247	B	B	2009	Manufacturing	Manufacturing;	Business Application
10248	A	A	2012	Communication	Telecommunications;	Business Application
10249	A	B	2006	Government	Government;	Business Application
10273	B	B	2009	Manufacturing	Manufacturing;	Business Application
10323	A	A	2002	Insurance	Insurance;	Business Application
10332	B	B	2009	Manufacturing	Manufacturing;	Business Application

Fig. 5. A Sample Part of ISBSG Dataset

As seen from Table 1, most of the proposed concepts can be mapped to those in existing ISBSG dataset. To better demonstrate the difference of the proposal with respect to the current operation, the following example changes can be made while mapping ISBSG dataset to the proposed model:

- The project information pool will include all rows but as allowed by data owner for a specific type of data user.
- Verifiers will be selected from data owners having similar project attributes.
- Role-based token will be defined to enable all roles to benefit from the system.
- Decentralized and attribute-based access control mechanism will be implemented with smart contracts on blockchain.

4 Discussions

The proposed solution should be considered in three levels; strategic, tactical and operational. Currently we are dealing with the issues of operation. Next, tactical and strategic issues need to be addressed. For example, there is a need for a standard data model for software project estimation which is of tactical level, and the data owned can be processed/mapped with respect to this data model by smart contracts.

On the level of operation, there may be limitations (or unexpected alternative flows) of the example scenario in realization. For example, if the data user is malicious in step 5.a, after project information is displayed to him/her, the user can copy project information (e.g. by taking an image of it) and share it with other people who do not have access rights. To address this problem, project information pool can be utilized in a way not to display project information but the result of the user operation. More specifically, the data user can define an operation (e.g., an estimation function) on system and run that operation on queried project information. The data user can then get only the result of the operation without seeing the information that led to that result. The limitations like this one will be elicited and discussed with actual stakeholders of the system in our upcoming studies, and the use case definitions will be revised accordingly prior to implementation.

Determining the blockchain technology to be used for a system using this model is a critical decision. The basic requirement of the model, i.e., the restricted access control, implies that private blockchains with more features in this respect are more suitable than public blockchains. Hyperledger technology, which is widely used among private blockchain technologies and supports smart contract implementation, will be the right choice for this model.

5 Conclusion

In this paper, we proposed a conceptual model for blockchain-based software project information sharing to encourage stakeholders for sharing and using project information by defining an access control mechanism. In order to make stored project information more reliable, an incentive mechanism that benefits all roles is employed. The features of blockchain technology make the model more secure and reliable.

This infrastructure will not be specific to project information, and it can be adapted for other kind of information sharing and storage problems. This work can be beneficial for companies that need to make estimations with software project data and for organizations, which want to make comparisons with software project information, like research centers, technology transfer offices etc.

In our upcoming work, by using the proposed model, a system will be designed and implemented. Following that, an empirical study is planned with a research center in order to evaluate operational principles and validate the usability of the model.

Acknowledgement

The authors would like to thank to TUBITAK BILGEM Advanced Technologies Research Institute (ILTAREN) for their support of the first author, and Hacettepe University for their support of the second and the third authors in this work.

References

1. Kitchenham, B., Mendes, E., Travassos, G. H.: Cross versus within-company cost estimation studies: A systematic review. In: Software Engineering, IEEE Transactions on, vol. 33, no. 5, pp. 316–329 (2007).
2. Turhan, B., Mendes, E.: A Comparison of Cross-Versus Single-Company Effort Prediction Models for Web Projects. In: 40th Euromicro Conference Series on Software Engineering and Advanced Applications, SEAA 2014. 285-292. 10.1109/SEAA.2014.41 (2014).
3. Idri, A., Amazal, F.,Abran, A.: Analogy-based software development effort estimation: A systematic mapping and review. In: Information and Software Technology. 58. 10.1016/j.infsof.2014.07.013 (2014).
4. Desharnais, J.M.: Analyse statistique de la productivitie des projects informatique a partie de la technique des point des function, PhD thesis, Univ. of Montreal (1989).
5. Desharnais dataset, http://promise.site.uottawa.ca/SERepository/datasets/desharnais.arff, last accessed 06.05.2019.
6. ISBSG, International Software Benchmarking standards Group, http://www.isbsg.org.
7. Boehm, B.W., Software Engineering Economics, Prentice Hall PTR, New Jersey (1981).
8. COCOMO dataset, http://promise.site.uottawa.ca/SERepository/datasets/cocomo81.arff, last accessed 06.05.2019.
9. QSM Software Project Database, https://www.qsm.com/resources/qsm-database, last accessed 23.06.2019.
10. QSM SLIM-Estimate, https://www.qsm.com/tools/slim-estimate, last accessed 23.06.2019.
11. QSM SLIM-Metrics, https://www.qsm.com/tools/slim-metrics, last accessed 23.06.2019.
12. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf, last accessed 06.05.2019.
13. Infographic: A Look at Blockchain Technology [Online Image]. Retreived 16.06.2019 from https://burniegroup.com/infographic-a-look-at-blockchain-technology
14. Ethereum. Blockchain App Platform. https://ethereum.org , last accessed 06.05.2019.
15. Hyperledger. Blockchain Technologies for business. https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf, last accessed 17.06.2019.
16. Azaria, A., Ekblaw, A., Vieira, T.,Lippman, A.: MedRec: Using Blockchain for Medical Data Access and Permission Management. In: 2nd International Conference on Open and Big Data (OBD) pp. 25-30, (2016).
17. Cruz, J.P., Kaji, Y.: The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication. In: The Third International Conference on Building and Exploring Web Based Environments (WEB), At Rome, Italy (2015).
18. Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. In: IEEE Access, vol. 5, pp. 14757-14767, (2017).
19. Cruz, J. P., Kaji, Y., Yanai N.: RBAC-SC: Role-Based Access Control Using Smart Contract. In: IEEE Access Volume 6, 12240-12251 (2018).
20. Liu, K., Desai, H., Kagal, L., Kantarcioglu, M.: Enforceable Data Sharing Agreements Using Smart Contracts (2018). https://arxiv.org/pdf/1804.10645.pdf, last accessed 06.05.2019.
21. Özyilmaz, K.R., Doğan M., Yurdakul A.: IDMoB: IoT Data Marketplace on Blockchain. In: Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 2018, pp. 11-19 (2018).

22. Trón, V., Scher, A., Nagy, D.A., Felföldi Z., Johnson, N.: Swap, Swear and Swindle: Incentive system for Swarm. (2016), https://swarm-gateways.net/bzz:/theswarm.eth/ethersphere/orange-papers/1, last accessed 06.05.2019.
23. Kabi, O.R., Franqueira, V.N.L.: Blockchain-Based Distributed Marketplace. In: Abramowicz W., Paschke A. (eds) Business Information Systems Workshops. BIS 2018. Lecture Notes in Business Information Processing, vol 339. Springer, Cham (2018).