# Blockchain Enabled Distributed Storage and Sharing of Personal Data Assets

Jānis Grabis
*Management Information Technology*
*Riga Technical University*
Riga, Latvia
grabis@rtu.lv

Vlado Stankovski
*Department of Computer Science*
*University of Ljubljana*
Ljubljana, Slovenia
Vlado.Stankovski@fri.uni-lj.si

Roberts Zariņš
*Management Information Technology*
*Riga Technical University*
Riga, Latvia
roberts.zarins@gmail.com

***Abstract*—Personal data are important information assets. Data sharing has potential of creating value to data owners as well as causing security and privacy concerns. Distributed storage solutions have emerged as an approach adhering to the Privacy-by-Design principles and in combination with blockchain technologies enable data and value exchange within communities of Internet users. The paper elaborates an approach for efficient distributed data storage and sharing, where access control is provided using the blockchain technologies and data searching and retrieval are facilitated using a knowledge base. A conceptual model and data management processes are elaborated and a prototype is developed. The prototype is used in experimental studies to compare data storage usage and data retrieval speed for the proposed approach and on-chain storage.**

***Keywords—personal data, privacy-by-design, distributed storage, blockchain, smart contracts***

## I. INTRODUCTION

Internet and World Wide Web have enabled massive distribution and sharing of data including personal data. Data sharing has potential of creating value to their consumers as well as their owners. However, Internet users have realized that unlimited sharing of the personal data could lead to security breaches. The personal information assets can be managed in a centralized or decentralized manner. In the former case access to information is often controlled by service providers and the individuals are not completely confident about the destiny of their data. Additionally, the individuals might have limited opportunities for benefiting from sharing their personal data. Decentralized and distributed storage solutions are designed without a single point of control [1]. Similarly, blockchains and smart contracts have emerged as technologies enabling information and value exchange in distributed environments [2]. Moreover, distributed cloud storage solutions should allow the individuals to deal with large volumes, velocity and veracity of the data [3]. In this respect, it is paramount to achieve high Quality of Service for distributed cloud storage operation. Unfortunately, blockchains have limitations concerning both storage volume and information processing speed.

The objective of this paper is to elaborate a method for efficient distributed storage and sharing of personal data assets within a community of users. The individuals should have a complete control over the way personal data are used and opportunity to benefit from sharing these data. The personal data are stored in a distributed storage and the individuals may choose which storage to use. The access to these data is controlled using a blockchain and smart contracts define access conditions. To improve data retrieval efficiency a concept of knowledge base is used. The knowledge base defines communities of the users and facilities information search operations. The privacy by design principles [4] are followed to ensure that the distributed personal data storage and sharing solution referred as to MyDataExperience adheres to users' privacy and information sharing needs.

The conceptual model of MyDataExperience as well as algorithms for data storage, sharing and searching are elaborated. A prototype of the solutions is implemented and used to evaluate data management efficiency. The Ethereum blockchain and InterPlanetary File System are used in the implementation. The evaluation objective is to compare the proposed solution with the on-chain storage of personal data according to the data storage usage and retrieval speed.

The main research contributions are:

- Blockchain controlled access to distributed personal data according to conditions specified in smart contracts;
- Development of the knowledge base as a mediator for efficient querying distributed personal data in combination with the blockchain technology to control access of personal data and to meet high Quality of Service requirements.

The rest of the paper is organized as follows. Section II analyzes suitability of the proposed solution from the perspective of the Privacy by Design principles and reviews related work. Section III describes design and implementation of the MyDataExperience personal data storage. Experimental evaluation of the proposed solution is reported in Section IV. Section V concludes.

## II. BACKGROUND

The adoption of the distributed storage controlled using blockchain technologies is driven by the need to adhere to the

2473-3490/20/$31.00 ©2020 IEEE
DOI 10.1109/ICDEW49219.2020.00-13

Privacy-by-design principles. The knowledge based information retrieval is introduced to address the efficiency concerns.

### A. Privacy-by-design and blockchains

The privacy-by-design principles were to ensure that applications are developed having users' privacy and security needs as the most significant priority. These principles are [4]:

1. Proactive not Reactive and Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

If centralized and decentralized personal data storage solutions are compared then these principles are better met by decentralized and distributed storage solutions (Table I).

TABLE I. EVALUATION OF CENTRALIZED AND DECENTRALIZED STORAGE SOLUTIONS ACCORDING TO PRIVACY-BY-DESIGN

| Principle | Centralized | Decentralized |
|---|---|---|
| Proactive not Reactive | Permissions are often imposed upon owner's request | Owner specifies permissions upfront and ownership is validated |
| Privacy as the Default Setting | Service provider defines permissions to select form | User specifies permissions |
| Privacy Embedded into Design | Assumption of trustworthiness; main emphasis on performance | Assumption of trustless environment |
| Full Functionality | Service provider benefits | Owner benefits |
| End-to-End Security | Points-of-failure | Security of assets, meta-data and tokens |
| Visibility and Transparency | Limited trace | Full trace |
| Respect for User Privacy | Courtesy of service provider | User requirements first |

However, the decentralized and distributed approach causes its own challenges concerning trust and value exchange which can be addressed using blockchain technologies. Wust and Gervais [5] proposed an algorithm to determine suitability of blockchains for particular needs. The evaluation shows that distributed personal data storage has following features:

- Needs to store states;
- Have multiple writers;
- Does not have always online trusted third party;
- All writers are not known;
- All writers are not trusted;
- Public verifiability is required.

As a result the permissionless blockchain is suitable for distributed personal data storage and community based sharing. However, the blockchain alone does not address all aspects important distributed personal data storage and full functionality cannot be achieved. Smart contracts can be used for these purposes. They key features important to distributed personal data storage and sharing possibility to exchange assets, dispute-less and self-enforcement.

### B. Related Work

Zyskin et al. [6] published one of pioneering woks on application of blockchain in personal data management. Similarly, blockchains can be used to control access to personal data [7,8]. However, there are couple of limitations to use blockchains for personal data management at scale. Singh and Lee [9] analyze non-functional characteristics and conclude that there are issues concerning flexibility, performance and cost efficiency. Kosteka et al. [10] add to this list latency, security and usability among others. Pongnumkul et al. [11] estimate that transaction execution latency increases exponentially with the increasing number of transactions and is several minutes long what is not acceptable for personal data management purposes. Ibanez et al. [12] analyze annotating of bitcoin transactions and indicate that limited memory is significant shortcoming. If blockchains are used for personal information then size of the blockchain becomes even more significant issue what will be resolved by using the blockchain for controlling access rather than for storing personal data themselves. The similar approach has been suggested in [13]. Blockchains enable development of GDPR compliant data exchange solutions [14]. Recognizing shortcoming of data retrieval from blockchains, recently, there has been and increasing interest in query languages for blockchains [15]. They add ability to perform range queries on top-k queries on the blockchain. Bartoletti et al. [16] develop analytical queries for analyzing cryptocurrency transactions.

Recently, the blockchain technology has been used jointly with distributed storage to provide unlimited storage capacity by combining on-chain and off-chain capabilities [17, 18]. These papers share similarity with the MyDataExperience approach, which mainly differs by introducing the knowledge base concept to facilitate data management processes.

## III. DESIGN

### A. Overview

The overview of the MyDataExperience personal data management solution is given in Fig. 1. A user who owns an asset (e.g., a picture) uses the solution to comprehend potential threats and benefits of sharing this asset with related entities (e.g., friends, companies willing to consume data). The asset is stored in a distributed storage, indexed in a knowledge base and a smart contract governing the asset usage is written into the blockchain. The asset is also indexed in knowledge bases owned by the related entities. The knowledge base contains the list of user and their addresses, access rights (relations among users and files), relations among the users (e.g. friendship relationships) and file usage data. The related entities or friends query the knowledge base to search for available assets. If conditions defined in the smart contract are validated, the blockchain provides access to the assets and the owner is compensated for data sharing using tokens.

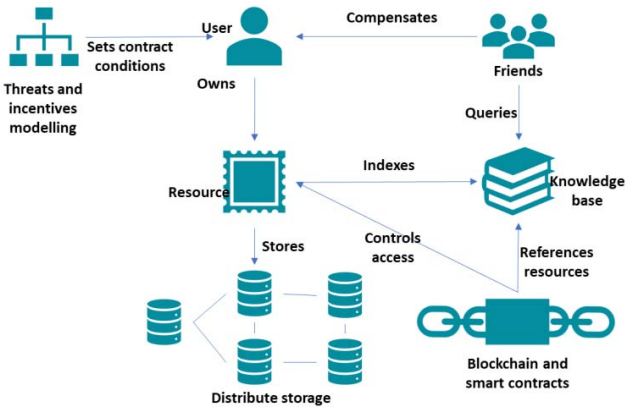


Fig. 1. Interactions among key elements of the `MyDataExperience` personal data management solution.

### *B. Data Management Processes*

The MyDataExperience solution allows users to perform these core data management processes:

- Store personal data assets in distributed storage;
- Share personal data assets taking into account privacy preferences;
- Search of personal assets shared by related entities.

To store personal data assets, a user interacts with the MyDataExperience front-end and data files representing the assets are submitted to the knowledge base (Fig. 2). The knowledge based identifies appropriate storage (that could include selection of the most suitable storage according the user's preferences) and establishes a connection to the distributed storage service. The assets are stored in the distributed storage and a reference to the asset is obtained. This reference is stored in the blockchain, which requires a payment for the transaction. Both public and private blockchains could be used. The private blockchain could be used to reduce costs or to create a personal data sharing economy. Once the payment is made, the assets' storage is confirmed.

The sharing process allows users to share their personal data assets with friends as well as other parties subject to data access conditions. The friends are users with whom the data owner has established relations in the data sharing community and data access is governed for the group as a whole rather than on the case to case basis.

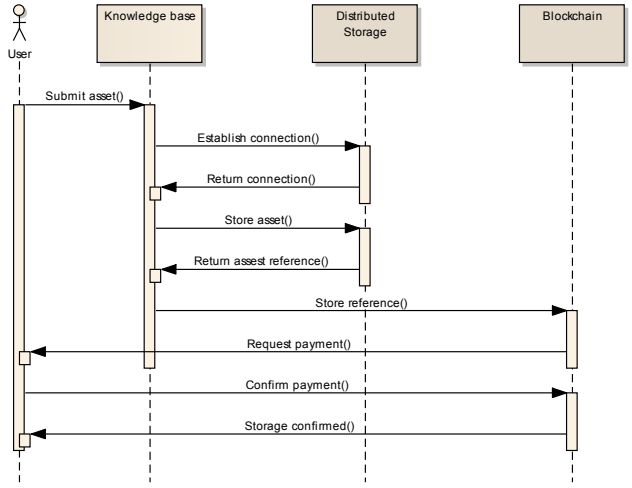


Fig. 2. Storing process.

In concert with her security preferences and expected sharing benefits, a data owner defines a smart contract describing conditions for sharing of resources. The smart contract is deployed in the blockchain (Fig. 3). A new blockchain transaction is executed with a change of the access rights. A friend can request access to the known asset (i.e., with a known reference without searching). The request is evaluated according to the smart contract stored in the blockchain. If it is a valid request, a new transaction including payment is created and the friend receives the access to the requested asset. The asset itself is retrieved from the distributed storage.

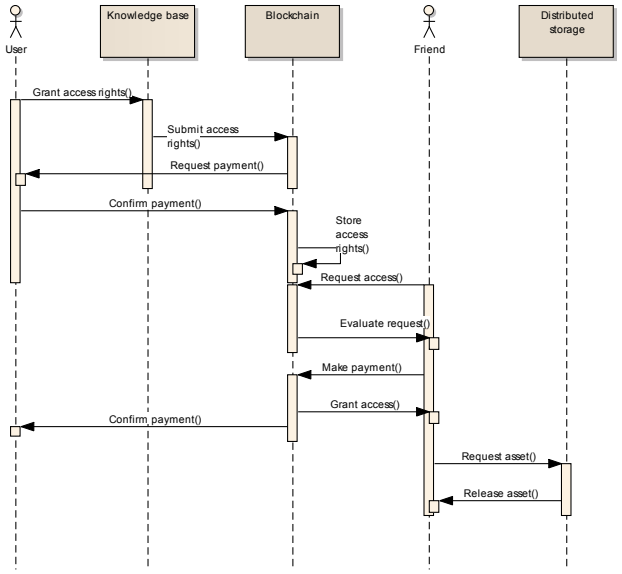


Fig. 3. Sharing process.

The search process (Fig. 4) is used by data consumers to find available personal data assets. The search can be performed by friends as well as other parties and using various search criteria such as assets' name, type and owner. Assets are searched in the knowledge base according to the search criteria

provided. The access rights to the assets are validated against the blockchain. The knowledge base returns to the user a list of the relevant and accessible assets. The user indicates the assets she would like to retrieve what triggers delivery of these assets from the distributed storage.

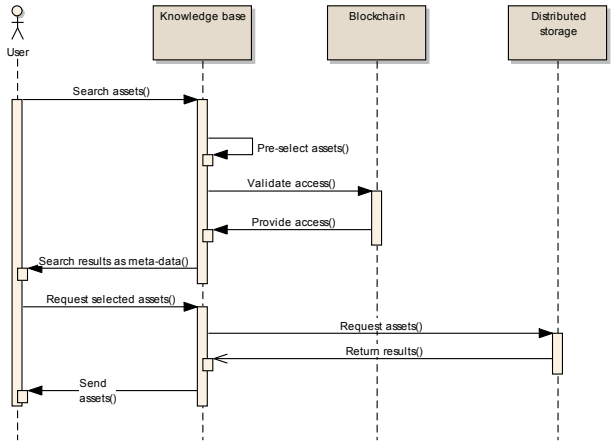


Fig. 4. Searching process.

The user searches the knowledge base for the resources in her neighborhood (e.g., shared by friends) and depth of the neighborhood can be controlled. The accesses right and sharing conditions for the requested resources are evaluated by retrieving this information from the blockchain for the pre-selected resources. This information is returned to the user who selects resources fitting her needs and means. This process could be fully automated. The MyDataExperience querying service mediates retrieval of the selected resources from the distributed knowledge and execution of the smart contracts is triggered on the blockchain.

### C. Technology

The key components of the MyDataExperience prototype are front-end supporting user interactions, distributed storage, blockchain with smart contracts and knowledge base. The React [1] framework is used to develop the front-end as a standard web application although different types of front-ends could be used to access MyDataExperience functionality using API. Ethereum[2] blockchain is employed and the Ropsten[3] test network in particular, which is accessed with the help of Infura[4] API. Transactions are handled using Ethereum Wallet. A web application was also used to provide the knowledge base functionality. Smart contracts were developed using the Solidity programming language. InterPlanetary File System[5] (IPFS) provides distributed storage facilities.

The knowledge base currently is also implemented on-chain. This way it is also decentralized. However, that would reduce efficiency of the solution if there are many users and a large number of files.

[1] https://reactjs.org/
[2] https://ethereum.org/
[3] https://ropsten.etherscan.io/
[4] https://infura.io/
[5] https://ipfs.io/

Fig. 5 illustrates the results of data storage in the blockchain. The blockchain stores IPFS reference of the personal asset, its name (e.g., SSO.PDF) and the user reference. The assignment of the full access rights to the asset's owner is shown in Fig. 6, where the first value indicates the owner and the following array indicates the full access rights.

```
truffle(development)> contract.get().then((val) => console.log(val))
QmfBF4a7itUVLYcDKMZDhYnVhw3m5Rh1XnzCbg8SnzEyRS

truffle(development)> contract.ipfshashes(1).then((val) => console.log(val))
TypeError: contract.ipfshashes is not a function
truffle(development)> contract.ipfsHashes(1).then((val) => console.log(val))
[ BigNumber { s: 1, e: 0, c: [ 1 ] },
  'QmadvrtnpyVGKUBMNyX8kepwxsCy4wPPaDoqJY3UdjYRk7',
  'SSO.PDF',
  '0x0dD18429d91e4A91cE3Ec7b0dB89b6f8CE2D756B' ]

truffle(development)> contract.ipfsHashes(2).then((val) => console.log(val))
[ BigNumber { s: 1, e: 0, c: [ 2 ] },
  'QmfBF4a7itUVLYcDKMZDhYnVhw3m5Rh1XnzCbg8SnzEyRS',
  'tesla-roadster-red-electricity-cars-luxury.jpg',
  '0x0dD18429d91e4A91cE3Ec7b0dB89b6f8CE2D756B' ]

truffle(development)>
```

Fig. 5. Sample files referenced in the blockchain.

```
truffle(development)> contract.getUser("0x0dD18429d91e4A91cE3Ec7b0dB89b6f8CE2D756B
[ '0x0dD18429d91e4A91cE3Ec7b0dB89b6f8CE2D756B',
  [ '0x0000000000000000000000000000000000000000',
    '0xd268ebc987f340616dac0c4e0cb5e42d1911e352' ],
  BigNumber { s: 1, e: 0, c: [ 0 ] } ]

truffle(development)>
```

Fig. 6. Access right assigned to the owner of the resource.

The MyDataExperience front-end provides functions for listing files, file upload, management of the community (i.e., friends of the assets' owner) and searching files (Fig. 7). The figure shows that assets are added to the distributed storage along with user identification. The MetaMask[6] interface from the browser to Ethereum Wallet shows the payment for storage of the asset.

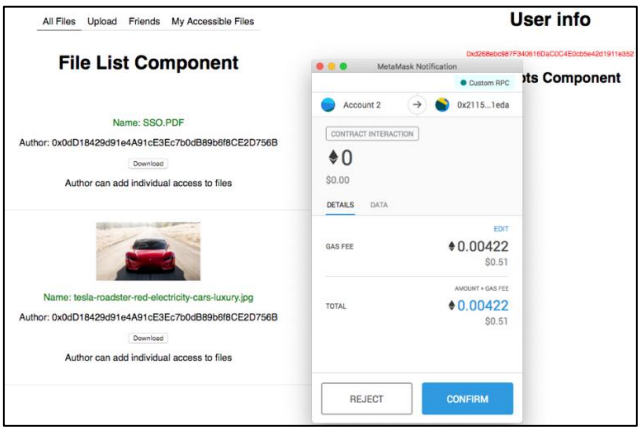


Fig. 7. The front-end of the MyDataExperience prototype.

## IV. Experimental

Experimental studies are conducted to evaluate the proposed personal data storage and sharing solution. The MyDataExperience is compared with plain storage of data

[6] https://metamask.io/

assets on-chain. The on-chain storage implies that files are stored directly in the blockchain rather in the distributed storage. The comparison is done according to the storage size and the data assets search efficiency.

### A. *Storage size*

The first set of experiments evaluates the storage utilization what is measured by the required storage size and cost of storage transactions in the Ethereum blockchain.

The cost of storage transactions in the Ethereum network is depends on the quantity of gas required to perform these transactions. The quantity of gas is determined by data volume and complexity of processing [26]. In the case of on-chain storage, the files are converted in hexadecimal format and stored in the blockchain. Three different files are used in the experiments (Table II). The files differ by their size and type.

TABLE II. FILES USED IN THE EXPERIMENTAL STUDIES

| File number | File type | Size, b |
|---|---|---|
| 1 | Text | 1024 |
| 2 | Image | 3219 |
| 3 | Image | 4720 |

During the experiment these three files were uploaded in the directly in the blockchain and MyDataExperience data storage. Table III shows the results of the experiment including:

- The size of the hexadecimal data string representing the file and stored in the blockchain in bytes;
- The total size of data stored in the blockchain including the file and access rights;
- Ethereum gas consumption to execute the transaction;
- Transaction costs in the *Ether* crypto-currency.

The results are independent of the file size in the case of the MyDataExperience solution, while the blockchain size and transaction cost increases linearly depending on the file size. This is illustrated in Fig. 8 showing the relative storage requirements between the on-chain and MyDataExperience cases. Obviously, the on-chain storage is significantly more expensive and more importantly it would lead to rapid increase of the blockchain size making it unusable.

TABLE III. THE RESULTS OF DATA STORAGE USAGE EXPERIMENTS

| File number | Hex file size, b | Total size, b | *Gas*, unit | Cost, Eth | BC size increase, b |
|---|---|---|---|---|---|
| On-chain | | | | | |
| 1 | 2048 | 2436 | 1622719 | 0,041 | 2436 |
| 2 | 6438 | 6852 | 4691848 | 0,117 | 9288 |
| 3 | 9440 | 9828 | 6762981 | 0,160 | 19116 |
| MyDataExperience | | | | | |
| 1 | 46 | 356 | 215089 | 0,005 | 356 |
| 2 | 46 | 356 | 215089 | 0,005 | 712 |
| 3 | 46 | 356 | 215089 | 0,005 | 1068 |

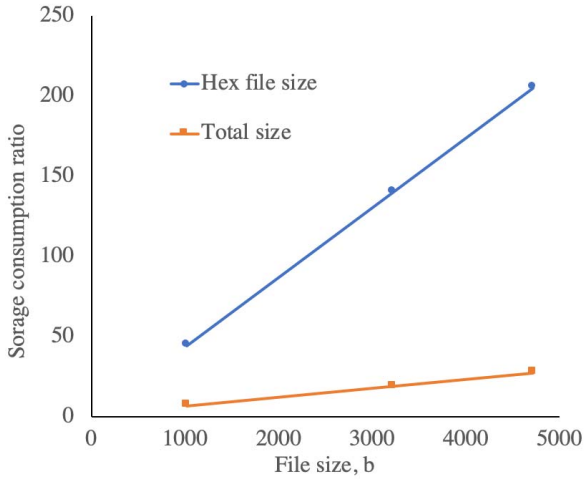


Fig. 8. Storage consumption ratio between the on-chain and MyDataExperience storage depending on the file size.

### B. *File search time*

The search time is also evaluated. Two search approaches are compared:

- On-chain retrieval – files are searched in the blockchain without the help of the knowledge base;
- MyDataExperience – files are searched using meta-data in the knowledge base and then retrieved from the blockchain.

There are several types of users in the MyDataExperience data sharing community. These types are distinguished from the data assets owner perspective. That includes: 1) data owner; 2) data owner's friend; 3) unrelated user who shares data with the owner; 4) unrelated user. The following users having the aforementioned types are created:

- 0xa7DefDF3BE5B556B0d7f3fB3de5aF05a4f6E1DF2 – owner;
- 0xd335B51d960061cC1FA145e6d4a1Fcf1aB55677C – first friend of the owner;
- 0xFAa18b9a1348eF8f9D66C77e1B19eD43D7912D3c – second friend of the owner;
- 0xA345c16b69bC7817FEDE586e460acbD7EC9aDAd5 – unrelated user who shares data with the owner;
- 0x4CDFF8CdeDeDe2b4117Ff0e416C44566dbbF3b97 – unrelated user.

Relations among these users are stored in the knowledge base. At the same time twelve different files were stored. The appropriate references and access rights were written in the blockchain. The file ownership referenced in the blockchain is shown in Table IV. Two files are uploaded by the owner herself. Six files are uploaded by the owner's friends (files 3 to 8). Three files are shared directly with the owner without establishing friendship. One file is uploaded by an independent user not related to the owner.

TABLE IV. FILE OWNERSHIP

| Nr | File | Owner |
|---|---|---|
| 1 | Object.json | 0xa7DefDF3BE5B556B0d7f3fB3de5aF05a4f6E1DF2 |
| 2 | SUSe.pdf | |
| 3 | CV.docx | 0xd335B51d960061cC1FA145e6d4a1Fcf1aB55677C |
| 4 | Twitter.jpeg | |
| 5 | Blockchain_Whitepaper.pdf | |
| 6 | Bird.jpeg | 0xFAa18b9a1348eF8f9D66C77e1B19eD43D7912D3c |
| 7 | Vote.pdf | |
| 8 | BC_diagram.xml | |
| 9 | Kvalifikacijas_prasibas.docx | 0xA345c16b69bC7817FEDE586e460acbD7EC9aDAd5 |
| 10 | Google_app.png | |
| 11 | Object_2.json | |
| 12 | Location.jpg | 0x4CDFF8CdeDeDe2b4117Ff0e416C44566dbbF3b97 |

These files are used to test several file search scenarios (Table V). The scenarios used different search conditions including file sharing conditions, friendship conditions, file type and file name.

TABLE V. FILE SEARCH SCENARIOS

| Nr | Scenario |
|---|---|
| 1 | Find all files owned by friends |
| 2 | Find all files owned by the user herself |
| 3 | Find all files shared with the user |
| 4 | Find all PDF files owned by friends |
| 5 | Find all files titled "Blockchain_Whitepaper" and owned by friends |
| 6 | Find all files owned by friend 0xd335B51d960061cC1FA145e6d4a1Fcf1aB55677C |

The scenarios are executed by searching files directly in the blockchain (files themselves are stored in the distributed storage) without using the knowledge based and by searching files in using the knowledge base and retrieval of the relevant files only. The search execution time including the data retrieval time is reported in Table VI and it is graphically illustrated in Fig. 9. The usage of the knowledge base in the MyDataExperience solution significantly reduces the search results. The search results depend only on the number of files returned and does not depend on the search criteria. In the case of on-chain search, the execution time depends on the search criteria because multiple conditions should be checked in the blockchain data.

TABLE VI. EXECUTION TIME OF THE FILE SEARCH SCENARIOS

| Search type | Scenario | Execution time, s |
|---|---|---|
| On-chain | 1 | 9 |
| | 2 | 10 |
| | 3 | 8 |
| | 4 | 14 |
| | 5 | 13 |
| | 6 | 19 |
| MyDataExperience | 1 | 3 |
| | 2 | 2 |
| | 3 | 3 |
| | 4 | 3 |
| | 5 | 3 |
| | 6 | 4 |

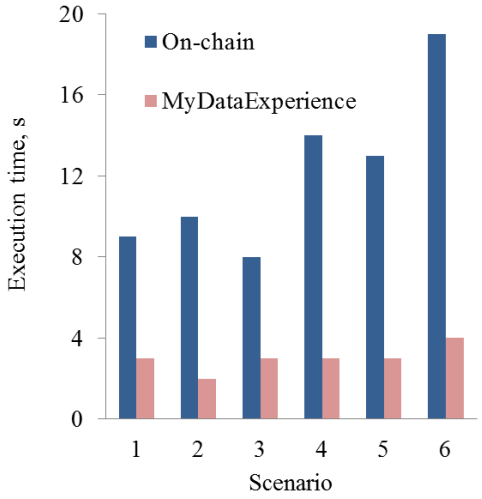


Fig. 9. Execution time of the File Search Scenarios.

## V. CONCLUSION

The distributed personal data storage and sharing solution has been developed in the paper. It is show to adhere to the principles Privacy-by-design and provides its users a full complete control on the way personal data assets are stored and shared in the community of users. The knowledge base referencing the data assets is used to facilitate their search process.

The proposed solution has been compared with on-chain storage and search. It has been shown that the MyDataExperience solution requires less storage space and is less expensive than the on-chain storage. The storage space is not dependent on the size of files stored. Additionally, utilization of the knowledge base expedites the search process.

The experiments were performed using small number data assets what was sufficient to demonstrate differences between the on-chain and MyDataExperience solutions but not sufficient to evaluate performance of the MyDataExperience solutions in high load situations. That will be addressed in further studies. The cost of maintaining the knowledge base in the distributed mode is also not investigated in this paper and is subject of further research. The knowledge base is currently implemented on-chain what would become a bottleneck as the size of the network grows. The knowledge base itself could be redeveloped by using the MyDataExperience approach by combining on-chain and off-chain solutions.

It is also envisioned that the solution should be made more user friendly. In particular, definition of smart contracts will be done in a model-driven manner. That will allow any user to specify her privacy considerations and willingness to benefit from personal data sharing. These preferences would be used to create smart contracts balancing privacy concerns and potential monetary gains from data sharing.

## REFERENCES


[1] S. Sakr, A. Liu, D.M. Batista, and M. Alomari, "A survey of large scale data management approaches in cloud environments," IEEE Communications Surveys and Tutorials, vol. 13, no. 3, 2011, pp. 311-336.

[2] N. Fabiano, "Blockchain and data protection: The value of personal data," IMCIC 2018 - 9th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings, 2018, pp. 112-115.

[3] V. Stankovski and R. Prodan, "Guest Editors' Introduction: Special Issue on Storage for the Big Data Era," Journal of Grid Computing, 16, 2018, pp. 161-163.

[4] A. Cavoukian, and M. Dixon, "Privacy and Security by Design: An Enterprise Architecture Approach," 2013, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

[5] K. Wust and A. Gervais, "Do you need a Blockchain?" Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 45-54.

[6] G. Zyskind, Nathan, O. and Pentland, A.S., "Decentralizing privacy: Using blockchain to protect personal data", Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, pp. 180-184.

[7] A. Kalra, Hasnain, S.S., Bodorik, P. and Jutla, D., "Access control mechanism using ethereum blockchain," 26th International Conference on Software Engineering and Data Engineering, SEDE 2017, pp. 107.

[8] D. Di Francesco Maesa, Mori, P. and Ricci, L. "Blockchain based access control", IFIP International Conference on Distributed Applications and Interoperable Systems, 2017, pp. 206-220.

[9] I. Singh, and Lee, S.-. "Comparative requirements analysis for the feasibility of blockchain for secure cloud," Communications in Computer and Information Science. Volume 809, 2018, pp. 57-72

[10] B. Koteska, Karafiloski, E. and Mishev, A., "Blockchain implementation quality challenges: A literature review", CEUR Workshop Proceedings, 2017.

[11] S. Pongnumkul, Siripanpornchana, C. and Thajchayapong, S. "Performance analysis of private blockchain platforms in varying workloads," 2017 26th International Conference on Computer Communications and Networks, ICCCN 2017.

[12] L.D. Ibanez, Fryer, H, et al. "Attaching Semantic Metadata to Cryptocurrency Transactions," Proceedings of the Workshop on Decentralizing the Semantic Web 2017 co-located with 16th International Semantic Web Conference, 2017, pp. 1-18.

[13] X. Xu, C., Pautasso, L. Zhu et al. "The Blockchain as a Software Connector". Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference, 2016, pp. 182-191 .

[14] R. Neisse, Steri, G. and Nai-Fovino, I., "A blockchain-based approach for data accountability and provenance tracking," ACM International Conference Proceeding Series, 2017, pp. 1-10.

[15] Y. Li, Zheng K. et al., "EtherQL: A Query Layer for Blockchain System," International Conference on Database Systems for Advanced Applications, DASFAA 2017: Database Systems for Advanced Applications, 2017, pp 556-567.

[16] M. Bartoletti, Lande, S., Pompianu, L. and Bracciali, A. "A general framework for blockchain analytics," SERIAL 2017 - 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Colocated with ACM/IFIP/USENIX Middleware 2017 Conference, 2017, pp. 1-6.

[17] M. Alessi, A. Camillò, E. Giangreco, M. Matera, S. Pino, and D. Storelli, "A decentralized personal data store based on ethereum: Towards GDPR compliance," Journal of Communications Software and Systems, vol. 15, no. 2, 2019, pp. 79-88.

[18] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, 2018, pp. 38437-38450.