The 13th KIPS International Conference on Ubiquitous Information Technologies and Applications (CUTE 2018) & The 10th International Conference on Computer Science and its Applications (CSA 2018)

December 17-19, 2018
Kuala Lumpur, Malaysia

Organized by

KIPS CSWRG

KIPS
Korea Information Processing Society

KIPS CSWRG
Korea Information Processing Society
Computer Software Research Group

The SA management scheme based on Blockchain for convergence service in S&T

YunHee Kang[1], R. Young Chul Kim[2], HeeSeok Choi[3]

[1] Div. of Information and Communication, Baekseok University
115 Anseo-dong, Cheonan Chungnam, Korea, 330-704
yhkang@bu.ac.kr
[2] Dept. of Software and Communications Engineering, 30016, Hongik University
bob@selab.hongik.ac.kr
[3] Convergence Service Center, KISTI
245 Daehak-ro, Yuseong-gu, Daejeon, 34141
choihs@kisti.re.kr

Abstract. A convergence service can be built by referring the specification of well-designed services and putting together them in bottom-up manner. In the service system for delivering an S&T convergence service, a service system needs to define a service agreement (SA) and to establish to support continuously and dependably the SA. In the paper we propose a SA management scheme that is used for storing the SA values co-created into the blockchain. The proposed scheme can provide a guideline for designing the S&T service system on SOA framework with a blockchain for providing information about SA as part of service metadata.

Keywords: SOA, service system, Service Agreement (SA), SA management scheme, Blockchain

1 Introduction

A convergence service can be built by referring the specification of well-designed services, and putting together them in bottom-up manner. Hence, we introduce a service integration model to deliver a service for convergence S&T knowledge infrastructure in a Service-oriented architecture (SOA) based on service platform so that it can easily meet the service agreement (SA) for them. The SA is a contract between a service provider and a service consumer [4, 5]. The contract includes the non-functional requirements of the service met between them.

In the service system for delivering an S&T convergence service, the service system needs to define SA, and to establish to support continuously and dependably the service agreement. Therefore, it is important to keep automatically the SA in the S&T knowledge infrastructure with services owned and managed by internal or external entities.

In the paper we propose the SA management scheme that is used for storing the SA values co-created into the blockchain. The scheme contributes to tackle its trustiness issue with a conflict among multi-parties by a smart contract between a service provider and a service consumer. The main contributions are listed as follows:

- design the core permissioned blockchain, and define its business models for the SA management
- design the metadata for services maintained by a distributed ledger for maintaining information about SA with transparency and traceability without interference of intermediary.

2 Related works

SOA is a strategic framework technology for designing and developing software in the form of interoperable service [5,6]. A service is defined as a unit of functionality that an entity (such as a system, organization, or department) makes available to its environment which has some value for certain entities in service users. SOA is a way to handle the growth of complexity of an enterprise software environment for providing a convergence service both a technical and a functional side.

Over the past several years, the blockchain technology has been driving a breakthrough in many domains including a p2p based distributed system, and introducing a business use case in diverse industries, including finance, real estate, healthcare, and transactive energy. This innovation rooted from the promise of Bitcoin [1,2], which is a p2p electronic cash operated to solve the double-spending problem without any intervention of a trusted intermediary. Bitcoin is the first application of blockchain. Blockchain provides specific properties (such as decentralization, transparency, and immutability) that have allowed Bitcoin to become a viable platform for "trustless" transactions by well-known techniques including cryptography, digital signature and consensus mechanism.

On the other hand, a blockchain platform, Ethereum, extended the capabilities of the Bitcoin blockchain by adding a new feature, smart contract [3]. A smart contract is a program that directly controls the exchanges or redistributions of digital assets between two or more members according to certain rules or conditions confirmed between involved members. It provides a single version of truth where participants use digitally signed blocks and consensus algorithms to alter transactions and documents using further blocks.

A blockchain is a decentralized system platform that maintains chronically a list of transactions grouped into blocks constructed via a consensus mechanism to keep information consistently. Figure 1 shows a block consists of a set of four transactions, t0 to t3, where t0 is happened before t1 and t3 occurs lastly in the causal relationship. As shown in Figure 1, SA represented as a digital asset is inputted to a hash function, H. The output of the hash function H is the hashed SA, SA´ that is used as a part of the transaction t2.

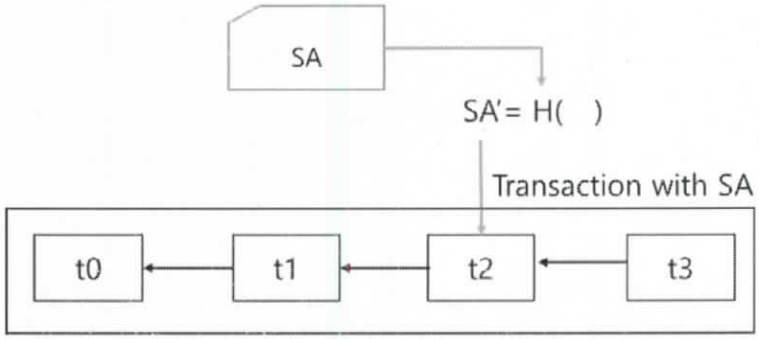

Fig. 1 a set of transactions in a block

One block can be added to the blockchain at a time. Each block is verified to ensure that it follows in sequence from the previous block. All SA transaction records are kept in the blockchain and are shared with peers, some members of a service system who have joined in a blockchain network. This decentralized process ensures properties of transparency, data integrity, and robustness.

3. The SA management scheme based on Blockchain

In this section, we design the service metadata for maintaining SA in a distributed ledger of a blockchain and the software architecture for blockchain based SA management scheme. The basic idea of our work starts from designing a SOA framework to enable the SA based requirements in publishing and discovery of services. The proposed scheme can provide a guideline for designing the S&T service system SOA framework with a blockchain for providing information about SA as part of service metadata.

By design, the blockchain is a decentralize technology. Blockchain technology has built-in robustness. Hence it may make types of record keeping like SA. By storing blocks of information that are identical across its network, the blockchain cannot be controlled by any single entity and has no single point of failure.

In a SOA structure, a service is a unit of work done by a service provider to achieve a useful result of performing some activities for a service consumer by a service request., Each service implements a specific business function and is made available such that the service can be accessed without knowledge of its underlying implementation. In a software context, services are typically thought of as methods, components, or building blocks of a larger automated system. In the service deliver process, there are three components such as service provider, service consumer and service broker that interact for delivering a specific server in asynchronous manner. There is the essential process of describing the service endpoint as a service metadata so that client can understand how to use the service.

The SA as a legal contract implies that each party to the agreement commits to providing the other party or parties with something they need or want. It underpins the joint understanding between a service provider and a service consumer of what to

expect from their mutual relationship. As shown Fig. 2, a service is delivered through the operation of a service system controlled by a service contract.

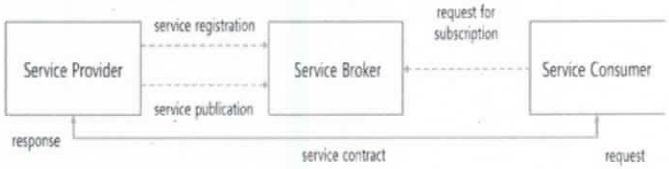

Fig. 2 Service deliver process

Table 1 shows the basic definition of the components of SA blockchain. SA is represented as a digital asset concerned in the blockchain. The participants of the blockchain, who the stakeholders of SA are, include a service consumer, a service provider and a service broker. In the SA blockchain, the transaction can be considered as three operations related with SA. To access the permissioned blockchain, Certificate Authority(CA) and X.509 is used for defining the format of public key certificates. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Table 1. The basic definition of the components of SA blockchain.

	Component	SA blockchain
1	Digital asset	Service agreement
2	Participant	Service provider Service consumer Service broker
3	Transaction	Read the current value of SA Read the defined SA value Write the value of SA updated
4	Access control	Read by Service provider Read by Service consumer Write by Service broker
5	ID management	CA and X.509 public/private key

The participants in the blockchain network should authenticate to add further changes in the transactions. It leverages a business ecosystem that represents several integrated business transactions for handling service agreement. The ledger is encryptions and available to all participants. A trusted intermediary is required for transactions related with SA between the service systems who wish to manage the quality of services. Blockchains allow us to have a distributed peer-to-peer network where non-trusting members, both a service provider and a service consumer can interact with each other without a trusted intermediary in a verifiable manner. Figure 3 shows the SA management scheme based on blockchain

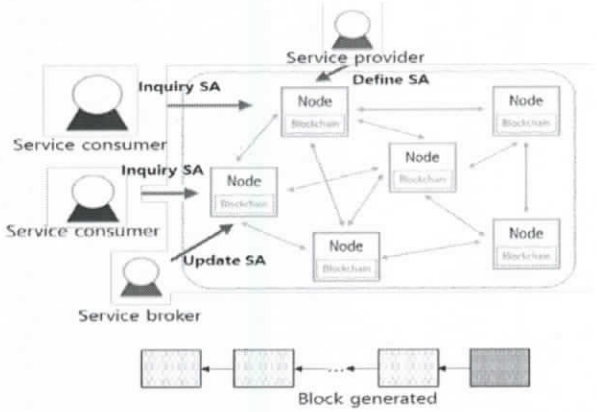

Fig.3 The SA management scheme based on blockchain

4. Conclusion

In this paper, the SA parameters have been managed by the SA management scheme based on blockchain for convergence service in S&T. This scheme is used for finding the service during services discovery process. The designed scheme is used as a reference architecture for construction of a prototype for verifying the integrity of SA ledger based on block and testing feasibility of the S&T knowledge infrastructure defined.

Acknowledgements. This Research was supported by the Korea Institute of Science and Technology Information(KISTI) in 2018

References

1. Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system
2. Swan, M. (2015). Blockchain : blueprint for a new economy. Sebastopol, Calif.: O'Reilly Media.
3. Szabo, N. Smart Contracts: Formalizing and Securing Relationships on Public Networks. First Monday, Volume 2, No. 9. 1997. Available online: http://firstmonday.org/article/view/548/46
4. Patrick Th, E., Rachid, G., Joe, S.: Distributed Asynchronous Collections: Abstractions for Publish/Subscribe Interaction. Proceedings of the 14th European Conference on Object-Oriented Programming, pp. 252-276. Springer-Verlag (2000)
5. François, A.R.J.: Software Architecture for Computer Vision: Beyond Pipes and Filters. Prentice Hall (2003)
6. Thomas Erl. 2005. Service-Oriented Architecture: Concepts, Technology, and Design. Prentice Hall PTR, Upper Saddle River, NJ, USA.

Message from the CUTE 2018 General Chairs

On behalf of the organizing committees, it is our pleasure to welcome you to the 13th International Conference on Ubiquitous Information Technologies and Applications (CUTE 2018), will be held in Kuala Lumpur, Malaysia on December 17-19, 2018.

This conference provides an international forum for the presentation and showcase of recent advances on various aspects of ubiquitous computing. It will reflect the state-of-the-art of the computational methods, involving theory, algorithm, numerical simulation, error and uncertainty analysis and/or novel application of new processing techniques in engineering, science, and other disciplines related to ubiquitous computing.

The papers included in the proceedings cover the following topics: Ubiquitous Communication and Networking, Ubiquitous Software Technology, Ubiquitous Systems and Applications, Ubiquitous Security, Privacy and Trust. Accepted papers highlight new trends and challenges in the field of ubiquitous computing technologies. We hope you will find these results useful and inspiring for your future research.

We would like to express our sincere thanks to Steering Committees: James J. Park (SeoulTech, Korea), Doo-Soon Park (SoonChunHyang University, Korea), Young-Sik Jeong (Dongguk University, Korea), Hsiao-Hsi Wang (Providence University, Taiwan), Laurence T. Yang (St.Francis Xavier University, Canada), Hai Jin (Huangzhong University of Science and Technology, China), Chan-Hyun Youn (KAIST, Korea), Jianhua Ma (Hosei University, Japan), Mingyi Guo (Shanghai Jiao Tong University, China), Weijia Jia (City University of Hong Kong, Hong Kong). We would also like to express our cordial thanks to the Program Chairs & Program Committee members for their valuable efforts in the review process, which helped us to guarantee the highest quality of the selected papers for the conference.

Finally, we would thank all the authors for their valuable contributions and the other participants of this conference. The conference would not have been possible without their support. Thanks are also due to the many experts who contributed to making the event a success.

CUTE 2018 General Chairs

Yi Pan, Georgia State University, USA
Sanghoon Kim, Hankyong National University, Korea
Luis Javier Garcia Villalba, Universidad Complutense de Madrid, Spain

Message from the CUTE 2018 Program Chairs

Welcome to the 13th International Conference on Ubiquitous Information Technologies and Applications (CUTE 2018), will be held in Kuala Lumpur, Malaysia on December 17-19, 2018.

The purpose of the CUTE 2018 conference is to promote discussion and interaction among academics, researchers and professionals in the field of ubiquitous computing technologies. This year the value, breadth, and depth of the CUTE 2018 conference continues to strengthen and grow in importance for both the academic and industrial communities. This strength is evidenced this year by having the highest number of submissions made to the conference.

For CUTE 2018, we received a lot of paper submissions from various countries. Out of these, after a rigorous peer review process, we accepted only high-quality papers for CUTE 2018 proceeding, published by the Springer. All submitted papers have undergone blind reviews by at least two reviewers from the technical program committee, which consists of leading researchers around the globe. Without their hard work, achieving such a high-quality proceeding would not have been possible. We take this opportunity to thank them for their great support and cooperation.

Finally, we would like to thank all of you for your participation in our conference, and also thank all the authors, reviewers, and organizing committee members. Thank you and enjoy the conference!

CUTE 2018 Program Chairs

Muhammad Khurram Khan, King Saud University, Kingdom of Saudi Arabia
Neil Y. Yen, University of Aizu, Japan
Yunsick Sung, Dongguk University, Korea