IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTELLIGENT SYSTEMS FOR THE INTERNET OF THINGS

Received October 29, 2017, accepted December 1, 2017, date of publication December 12, 2017,
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2782733

INVITED PAPER

BIDaaS: Blockchain Based ID As a Service

JONG-HYOUK LEE, (Senior Member, IEEE)
Department of Software, Sangmyung University, Cheonan 31066, South Korea
e-mail: jonghyouk@smu.ac.kr

This work was supported by the research grant from Sangmyung University.

ABSTRACT Blockchain technology has been known as the underlying technology of cryptocurrencies, but nowadays it is further considered as a functional technology for improving existing technologies and creating new applications previously never practical. In this paper, we are focused on utilizing blockchain technology to introduce a new ID as a service (IDaaS) for digital identity management. The proposed blockchain-based ID as a service (BIDaaS) is explained with one practical example that shows how the proposed BIDaaS works as an identity and authentication management infrastructure for mobile users of a mobile telecommunication company.

INDEX TERMS Blockchain, IDaaS, identity, authentication.

I. INTRODUCTION

Recently, we have seen a wide range of blockchain financial applications [1], [2] as well as an array of global companies adopting blockchain technology for various services [3]–[5]. Blockchain technology was first introduced as Bitcoin's underlying technology [6] but soon later its extendable capabilities have been recognized.

The peer-to-peer cryptocurrency, Bitcoin, is a core innovation in the financial sector nowadays. Its underlying technology, blockchain, is a type of a distributed ledger specially suitable for processing time ordered data. In addition, embedded cryptography functions of blockchain technology enable integrity of ledgers, authenticity of transactions, and privacy of transactions without a centralized control actor. Those make the blockchain different from traditional distributed database systems being used in the financial sector, e.g., it is practically impossible to modify or delete records of a ledger in the blockchain. This distributed and decentralized nature of the blockchain has attracted financial institutions over the world to replace existing backbone technologies with blockchain technology. For instance, according to [7], blockchain technology could save between US $5 billion and $10 billion in reinsurance thanks to improvements to placement, claims settlement, and compliance checks. Another example is a blockchain based stock exchange that will change share trading more dramatically without a centralized system.

Not only financial institutions are making these actions. Key companies in other sectors are adopting blockchain technology. For instance, the logistics sector considers blockchain technology for real-time visibility, improved efficiency, transparency, verifiability, and cost reduction for logistics. The property sector is adopting blockchain technology as well for digital but unforgeable property records, few disputes, transparency, verifiability, and lower transfer fees. The food sector is also investing blockchain technology to trace the movements of foods and tackle contamination faster.

In this paper, we consider blockchain technology as a new functional technology to create a new ID as a Service (IDaaS). A blockchain based ID as a Service (BIDaaS) is introduced with one practical example for mobile users of a mobile telecommunication company. In the proposal, there are three entities involved: user (e.g., mobile user), BIDaaS provider (e.g., telecommunication company), and partner of the BIDaaS provider (e.g., partner of the telecommunication company). Mutual authentication between the user and the partner is established without any pre-shared information or security credential shared among them. In other words, the user does not require any ID creation to the partner offering services to the user. The BIDaaS blockchain, where the BIDaaS provider and its partners have permissions to access, provides required information for IDaaS. Furthermore, the proposal allows the partner to selectively request other information of the user (e.g., real name, mobile phone number, postal address, etc.) from the BIDaaS provider.

The remainder of this paper is organized as follows: Section 2 presents a brief literature review about blockchains and demand for a new type of IDaaS. Section 3 presents the proposed BIDaaS with one practical example for mobile users of a mobile telecommunication company.

Some discussions are presented in Section 4. Section 5 concludes this paper.

II. PRELIMINARIES

A. BLOCKCHAINS

A blockchain is one type of a distributed ledger that consists of replicated, shared, and synchronized data over the Internet. The blockchain needs no centralized control actor or centralized data storage for maintaining its data. The first introduction of a blockchain was by Satoshi Nakamoto in 2008 and implemented as a core part of Bitcoin.

There are various blockchains with different goals (e.g., Bitcoin uses its own blockchain called Bitcoin blockchain [6], whereas Ethereum uses its own blockchain called Ethereum blockchain [8]) but the followings are common elements:

- Replicated ledger: The history of all transactions among nodes in a blockchain are securely stored. A block consists of transactions that are append-only with immutable past. The blocks are distributed and replicated among the blockchain nodes.
- Cryptography: Integrity of all transactions shared among the blockchain nodes is supported with digital signatures and specialized data structures (e.g., hash based data structure called Merkle tree [9]). Authenticity of transactions is supported with digital signatures. Privacy of transactions is also supported with anonymous addresses for transactions.
- Consensus: Transactions that are exchanged among the blockchain nodes over the Internet need to be validated before adding to the existing blocks. A consensus among the blockchain nodes is required for the validation. For a public blockchain, a representative consensus algorithm is Proof-of-Work (PoW) [6], which is used by Bitcoin. Practical Byzantine Fault Tolerance (PBFT) [10], [11] is a representative consensus algorithm used by HyperLedger Fabric [12] for a private blockchain.
- Peer-to-Peer networking: All transactions are shared without a centralized control actor over the Internet. In other words, the blockchain nodes are connected through a peer-to-peer network over the Internet, not through the client-server model, due to no trust entity involvement.

Blockchain technology also has some downsides. The blockchain ensures a strong degree of security for its chain (i.e., a set of blocks linked) but the risk of managing private keys exists. The private keys are used to prove ownership of a certain asset or data in the blockchain, but those keys could be lost or stolen by attackers. Another issue is scalability. As the blockchain is immutable and append-only, it must maintain a continuously growing list of blocks. For the Bitcoin blockchain, its size reached 100 GB on December 16, 2016 and continues to grow. Also there is an issue regarding the block size, e.g., how many transactions are included in one block. Network performance is also considered. The transactions per second is one of major performance factors that most of the blockchain implementations is trying to improve. As transactions need to be broadcasted to blockchain nodes connected through a peer-to-peer network, the network could be easily congested. Network congestion would be a critical issue with the growth in transactions and the limited block size.

B. DEMAND FOR A NEW TYPE OF IDaaS

Cloud computing has brought a massive change in the computing industry. Software, platform, and infrastructure can be provided to users as a service from a cloud nowadays. Identity management could be also provided from the cloud to a user. In other words, the user could use an identity and authentication management infrastructure provided from the cloud as a form of IDaaS. It would offer various benefits such as a reduced on-site infrastructure, integrated management with cloud services, and ease use. However, the use of IDaaS means outsourcing critical functions to a third party. All data related to identity and authentication (e.g., user account information, security credentials, etc.) is managed and controlled by the third party without knowing how the data is protected and processed on the cloud.

III. PROPOSED BLOCKCHAIN BASED ID AS A SERVICE

A. OVERVIEW

The proposed blockchain based ID as a Service (BIDaaS) is a new type of IDaaS. BIDaaS is designed for providing an identity and authentication management infrastructure from the BIDaaS provider to its partners. The involved three entities are as follows.

- BIDaaS provider: It is the BIDaaS provider to its partners.
- Partner: It is a partner of the BIDaaS provider. It normally has a service offering users.
- User: It is a user registered to the BIDaaS provider, but is not registered to services of the partner. The user wants to use a service offered by the partner, but the user may not want a creation of a new ID nor provide personal information to the partner for the service.

The BIDaaS provider maintains the BIDaaS blockchain, which is a private blockchain. The partner has access to the BIDaaS blockchain, but only a read permission, not a write permission. The BIDaaS provider writes a user's virtual ID, user's public key, etc. with a digital signature of them into the BIDaaS blockchain. Note that the signature is made with a private key of the BIDaaS provider.

The partner reads the user's virtual ID and user's public key information from the BIDaaS blockchain when the user requests to access its service with the virtual ID. The partner can confirm whether the claimed virtual ID from the user is the one registered in the BIDaaS blockchain by accessing the BIDaaS blockchain. If confirmed well, the partner begins the mutual authentication procedure for the user with the user's virtual ID and user's public key obtained from the BIDaaS blockchain.

Without preregistered information of the user to the partner's service, mutual authentication can be successfully

TABLE 1. Notations.

Notation	Definition
$\Im^{usr}$	Virtual ID of a user
K_{pri}^{usr}	Private key of the user
K_{pub}^{usr}	Public key of the user
K_{pri}^{pro}	Private key of a BIDaaS provider
K_{pub}^{pro}	Public key of the BIDaaS provider
K_{pri}^{ptn}	Private key of a partner
K_{pub}^{ptn}	Public key of the partner
$Sig_{K_{pri}}(\cdot)$	Signature with the private key K_{pri}
$E_{K_{pub}}(\cdot)$	Encryption with the public key K_{pub}
r	Nonce

done. After successful mutual authentication, the partner is only able to distinguish the user by the virtual ID. If the partner needs other information of the user, it would be possible to request the extra information (e.g., real name, mobile phone number, postal address, etc.) from the BIDaaS provider. The requested extra information is provided from the BIDaaS provider's user account database, not from the BIDaaS blockchain, through an pre-established secure channel between the partner and the BIDaaS provider.

B. PROCEDURES

The main procedures of BIDaaS are presented in this subsection. Used notations are listed in Table 1.

1) VIRTUAL ID CREATION

The user creates a pair of private key K_{pri}^{usr} and public key K_{pub}^{usr}. The user stores K_{pri}^{usr} safely. K_{pub}^{usr} is then used to create a virtual ID $\Im^{usr}$. The rule for generating $\Im^{usr}$ can be similar with the Bitcoin address generation, e.g., a cryptographic hash function over K_{pub}^{usr} is used to generate $\Im^{usr}$.

2) BIDAAS BLOCKCHAIN REGISTRATION

K_{pub}^{usr} and the generated $\Im^{usr}$ are securely transferred from the user to the BIDaaS provider. Note that a secure channel between the user and the BIDaaS provider is assumed. The BIDaaS provider creates a digital signature over K_{pub}^{usr} and $\Im^{usr}$, using its own private key K_{pri}^{pro}. The BIDaaS provider then registers K_{pub}^{usr} and $\Im^{usr}$ with the created signature $Sig_{K_{pri}^{pro}}(K_{pub}^{usr}, \Im^{usr})$ in the BIDaaS blockchain. This registration is performed as a blockchain transaction that is broadcasted to BIDaaS blockchain nodes. The registration is then stored at the BIDaaS blockchain.

3) MUTUAL AUTHENTICATION

When the user wants to access a service offered by the partner, the user only presents $\Im^{usr}$ with a nonce r to the partner by sending a message $M_1 = (\Im^{usr}, r, Sig_{K_{pri}^{usr}}(\Im^{usr}, r))$. When the partner receives the service access request from the user, it first accesses the BIDaaS blockchain to check if the presented $\Im^{usr}$ exists on the records of the BIDaaS blockchain or not. If existed, then the partner obtains the relevant information such as K_{pub}^{usr} and validates M_1. If well validated, the partner sends a message $M_2 = (\Im^{usr}, r+1, E_{K_{pub}^{usr}}(\Im^{usr}, r+1, K_{pub}^{ptn}))$. Upon receiving on M_2, the user decrypts the message with K_{pri}^{usr} and validates with $r+1$. As a successful result, the user obtains K_{pub}^{ptn} from M_2. The user sends a message $M_3 = (\Im^{usr}, r+2, E_{K_{pub}^{ptn}}(\Im^{usr}, r+2))$. As the partner receives M_3, it decrypts the message with K_{pri}^{ptn} and validates the message with $r+2$. Mutual authentication between the user and the partner is established thanks to the BIDaaS blockchain.

4) EXTRA INFORMATION REQUEST

The partner may request the BIDaaS provider some extra information required for providing its service to the user. For instance, if the partner is an online shopping mall, it thus requires at least the postal address of the user to deliver purchased items. The partner requests required information of the user via a separate secure channel established with the BIDaaS provider.

C. EXAMPLE

Fig. 1 shows how the proposed BIDaaS works as an identity and authentication management infrastructure for a mobile user of a mobile telecommunication company.

In this example, the mobile user wants to access an online shopping mall, which has a partnership with the mobile telecommunication company. As the mobile user's information is already registered at the mobile telecommunication company, the mobile user simply needs to generate its virtual ID and requests to register it with the corresponding public key into the BIDaaS blockchain. Note that the virtual ID registration can be done before the mobile user accesses the online shopping mall and multiple virtual ID pre-registrations are also possible.

The mobile user sends a service access request message to the online shopping mall. The message does not contain any real identity information of the mobile user, but a virtual ID of the mobile user is included. When the online shipping mall receives the request message, it looks up the BIDaaS blockchain with the provided virtual ID. As the online shopping mall has a partnership with the telecommunication company, which is the BIDaaS provider in this case, the online shopping mall can access the BIDaaS blockchain to get the necessary data for the provided virtual ID. The online shopping mall obtains at least the user's public key, which is valid and authentic, from the BIDaaS blockchain. Then, the online shopping mall uses the obtained user's public key for mutual authentication with the mobile user.

After authentication and service access approval, the online shopping mall may need some extra information of the mobile user such as the real name, mobile phone number, and postal address. Then, it can be obtained from the mobile telecommunication company's user account database.

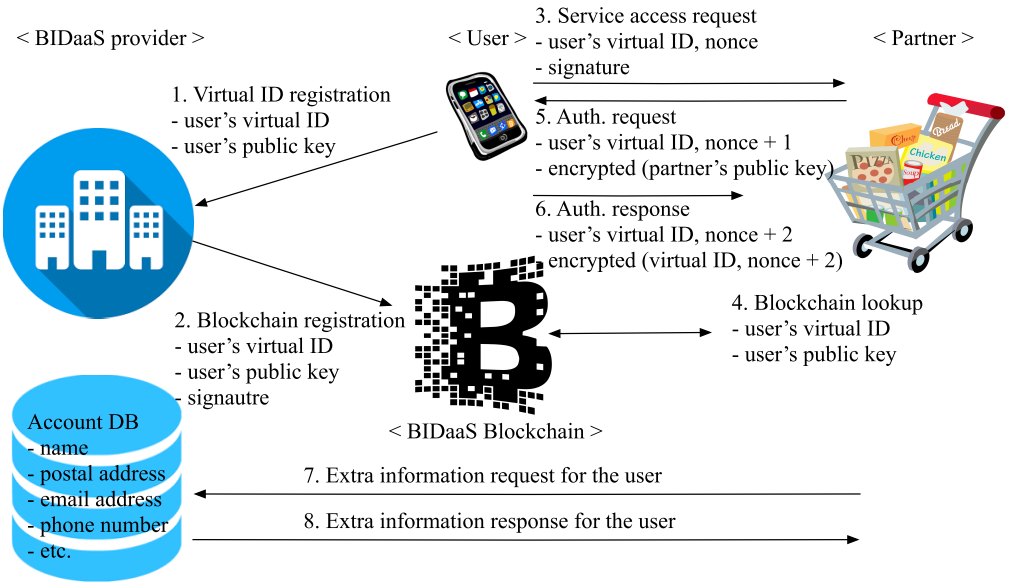

FIGURE 1. BIDaaS for a mobile user.

IV. DISCUSSION

A. CONSENSUS ALGORITHM

As the BIDaaS blockchain is a private blockchain, the PBFT algorithm can be used rather than the PoW algorithm, which requires a considerably high amount of computing power to reach a consensus on a block. The PBFT algorithm is based on replicated state machine and voting by replicas for state changes. Compared with the PoW algorithm, it is known as a lower computing power required, while providing embedded design optimizations such as reducing the size and number of messages exchanged between nodes.

B. CONSORTIUM BLOCKCHAIN

The BIDaaS blockchain in this paper is a private blockchain, which means that the BIDaaS blockchain is owned by the BIDaaS provider (e.g., mobile telecommunication company in our example), but it can be operated by consortium members (e.g., mobile telecommunication company and its partners in our example). However, it does not mean that the user account information is shared among all consortium members. In other words, the mobile telecommunication company still keeps its user account information and provides other partners if requested.

C. SERVICE LEVEL AGREEMENT

A service level agreement (SLA) may exist between the partner and the BIDaaS provider. This allows the BIDaaS provider creates new sources of revenue by providing a identity and authentication management solution as well as the extra user information to the partner. A SLA between the user and the BIDaaS provider may be also required as the BIDaaS provider supplies the user's personal information to the partner. For instance, in the mobile user case, when the mobile user subscribes to the mobile telecommunication company, the SLA between the user and the mobile telecommunication company (i.e., BIDaaS provider) can be established.

D. PROVIDED USER INFORMATION

Once the extra user information is provided to the partner, the provided user information is used by the partner. It means that the provided user information is not guaranteed to be used only for once. The partner may store and use for other purposes. For better user privacy, a scheme to detect or prevent misuse of the provided user information.

E. USE OF VIRTUAL IDs

The virtual ID may be used per service or per partner. Also, the same virtual ID may be used for all partners. It would be depending on the user's decision. The user may have a preference to use the virtual IDs, which are registered in the BIDaaS blockchain in advance. The preference may effect on a degree of user privacy as the same virtual ID can be tracked during the period of use.

F. TIMESTAMP INSTEAD OF A NONCE

The nonce is used during mutual authentication between the user and the partner, but it can be replaced with a timestamp. Nowadays, portable computing devices such as laptop and mobile phone that have a precise clock synchronization scheme are omnipresent.

G. PRIVATE KEY OF A USER

The user's private key must be safely stored and managed. For the mobile user, the private key may be stored at an electronic subscriber identity module (eSIM) and other sensitive information such as key generation materials are executed and stored at the trusted execution environment (TEE).

H. BENEFITS TO THE BIDaaS PROVIDER

The BIDaaS provider creates new sources of revenue by providing an identity and authentication management solution as well as providing existing user information to its partners.

I. BENEFITS TO THE PARTNER

The partner providing its service to the user does not need to implement and maintain an in-house identity and authentication management infrastructure. In addition, the partner is free from the burden of storing and managing securely sensitive user information. Necessary information of the user is pulled from the BIDaaS provider's user account database only when it is needed.

J. BENEFITS TO THE USER

The user does not need to create unnecessary accounts for services that the user may use for instance once a month. With a number of accounts for Internet services, the user is difficult to manage all the account information. For instance, it would be difficult to remember all the IDs and corresponding passwords. In addition, the user does not need to provide its personal information to various service providers.

V. CONCLUSION

This paper has presented a blockchain based ID as a Service (BIDaaS), which is a new type of IDaaS for identity and authentication management. Each procedure of the proposal has been described in details. In addition, one practical example showing how the proposed BIDaaS works as an identity and authentication management infrastructure for mobile users of a mobile telecommunication company has been presented.

As discussed, the proposed BIDaaS has a room for improvement. The first thing to consider is to develop a scheme to detect or prevent misuse of the provided user information at the partner. It can be implemented as a cloud platform that the partner is only granted to access for permitted services. The second is to develop a secure TEE operation for the mobile user case. The public and private key pair is generated at the mobile phone and besides private key is stored at the mobile phone. Today the TEE provides the most secure area that guarantees code and data loaded inside to be protected in terms of confidentiality and integrity.

REFERENCES

[1] F. Brezo and P. Bringas, "Issues and risks associated with cryptocurrencies such as bitcoin," in *Proc. 2nd Int. Conf. Soc. Eco-Informat.*, 2012, pp. 20–26.
[2] A. Gervais, G. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?" *IEEE Security Privacy*, vol. 12, no. 3, pp. 54–60, May/Jun. 2014.
[3] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 19–23, Jul. 2017.
[4] M. Pilkington, R. Crudu, and L. G. Grant, "Blockchain and bitcoin as a way to lift a country out of poverty—Tourism 2.0 and e-governance in the republic of moldova," *Int. J. Internet Technol. Secured Trans.*, vol. 7, no. 2, pp. 115–143, Oct. 2017.
[5] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, Mar. 2017.
[6] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.
[7] *Top Financial Services Issues of 2017*, PwC, London, U.K., Dec. 2016.
[8] G. Wood, "Ethereum: A secure decentralised generalized transaction ledger," Tech. Rep., 2014.
[9] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. Conf. Theory Appl. Cryptogr. Techn.*, 1987, pp. 369–378.
[10] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.
[11] A. Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, "Making byzantine fault tolerant systems tolerate byzantine faults," in *Proc. 6th USENIX Symp. Netw. Syst. Design Implement.*, 2009, pp. 153–168.
[12] C. Cachin, "Architecture of the hyperledger blockchain fabric," Tech. Rep., Jul. 2016.

JONG-HYOUK LEE (M'07–SM'12) received the Ph.D. degree in computer engineering from Sungkyunkwan University, Suwon, South Korea. In 2009, he joined INRIA, France, where he undertook the protocol design and implementation for IPv6 vehicular communication and security. He started his academic profession at TELECOM Bretagne, France, in 2012, as an Assistant Professor. In 2013, he moved to Sangmyung University, Cheonan, South Korea. His research interests include blockchain, malware analysis, and protocol analysis. He received the Best Paper Award at the IEEE WiMob 2012 and the Best Land Transportation Paper Award from the IEEE Vehicular Technology Society in 2015. He was a Tutorial Speaker at the IEEE WCNC 2013, the IEEE VTC 2014 Spring, and the IEEE ICC 2016. He was introduced as the Young Researcher of the Month by the National Research Foundation of Korea Webzine in 2014. He received the Haedong Young Scholar Award in 2017. He is an Associate Editor of the IEEE TRANSACTIONS on CONSUMER ELECTRONICS and *IEEE Consumer Electronics Magazine*. He is an author of the Internet Standards: *IETF RFC 8127* and *IETF RFC 8191*.