Commun.Fac.Sci.Univ.Ank.Series A2-A3
Volume 61, Number 1, Pages 102-110 (2019)
DOI: 10.33769/aupse.506181
ISSN 1303-6009 E-ISSN 2618-6462
http://communications.science.ankara.edu.tr/index.php?series=A2A3

DESIGNING A SECURE BLOCKCHAIN-BASED TRADING PLATFORM FOR INTERNET OF THINGS

Aydın ELBUZ, Murat OSMANOGLU and Omer Ozgur TANRIOVER

ABSTRACT. Blockchain, a distributed database technology attracts intensive attention recently. It was first described in 1991 by Stuart Haber and W. Scott Stornetta, in order to prevent tampering for document timestamps [1]. After that, Satoshi Nakamoto conceptualized this technology with his work, a peer-to-peer electronic cash system named as Bitcoin. Due to its authenticity, user anonymity and data immutability; this technology has also been applied to different areas ranging from finance, supply-chain managements to social services. In this paper, we propose a blockchain based application for trading data, collected from IoT devices. Our application enables the sellers to commercialize their data in exchange of the currency produced by the application. The application also utilizes smart contracts to establish trust between both sides of the exchange. Furthermore, we discuss the security and reliability of the system components.
.

1. INTRODUCTION

Blockchain is an efficient technology that realizes distributed ledger, which is a decentralized and publicly available data structure for storing transactions. These transactions are verified through a majority consensus [2,3]. So once the transactions are written in the ledger, they can't be changed and erased unless someone can take control majority of the system at the same time [4]. Blockchain is a read-only database system that makes it impossible to create and add a fraudulent or incorrect transaction to the chain. This feature presents a safe and secure system that eliminates third parties along with data immutability and user anonymity.

Bitcoin is the most popular application of blockchain and it took the world by storm when it showed up. After that, mostly in finance sector, many other similar implementations appeared that uses blockchain technology. Due to its success in finance, blockchain's popularity has surpassed these levels and spread in many

Received by the editors: January 01, 2019; Accepted: May 14, 2019.
Key word and phrases: Blockchain, internet of things, distributed ledger.

areas.

Internet of things (IoT) network was also affected from blockchain technology. IBM states that blockchain allows IoT to accelerate transactions and reduce the risk of collusion and tampering, which also reduces costs and complexity of operations [5]. Nowadays, this technology used for controlling and configuring IoT devices [6] and shared economy applications [7]. Besides, blockchain has also been used in smart buildings and food and pharmaceutical industries [8].

Huh, Cho and Kim [6] proposed a blockchain based solution for designing an IoT system. They aimed to control and configure IoT devices using the blockchain. The system uses RSA public key cryptography for managing keys. Private keys saved on individual IoT devices. Beside Ethereum platform is used for smart contracts and storing public keys. They simulated IoT system using Raspberry Pi devices and ran a Turing-complete code for smart contracts. However, they observed that the transaction time of Ethereum blockchain is slow. Thus, they needed a proxy or a large storage for saving entire blockchain because of Ethereum's light client protocol supporting issue.

Dorri et al. [9] proposed a tiered lightweight scalable blockchain, the optimized blockchain system, for IoT security and privacy requirements. They used a smart home setting for IoT applications. The system achieves decentralization by forming an overlay network where high resource devices jointly manage a public blockchain. The overlay designed as distinct clusters to reduce overheads. The cluster heads are responsible for managing the public blockchain. In conclusion, they observed that the lightweight scalable blockchain increases blockchain scalability compared to relevant baselines. It also resilient to some security attacks and it decreases packet overhead and delay.

In this paper, we introduce an application of blockchain to IoT data. Our application can be viewed as an extension of the construction introduced by Elbuz et al. [10]. It can be considered as a platform in which sellers can commercialize their data collected from an IoT device, and customers can contact with sellers, examine the data and buy it. This platform gives confidence to both seller and customer side. Our system uses blockchain technology together with smart contracts for reliability of data and secure money transfer.

The rest of the paper is organized as follows. Section II provides an overview of the used technologies. Section III describes the design of the proposed system and its scenario. Section IV analyzes the system and components' security. Finally, Section V concludes the paper and explains future works.

2. DEFINITION

In this section, we give the definitions of the core components that will be used to build our platform.

Cryptographic hash function is a one-way mathematical function or an algorithm which produces a unique fixed length string of text from a data or a file of an arbitrary length. Because the same data always results in the same hash, a small change to a data changes the whole hash value. And it is computationally infeasible to generate the data from its hash value due to the pre-image resistance feature. Also, cryptographic hash functions have collision resistance, i.e. it is very hard to find the same hash value from any two different inputs with any length.

Digital signature is a mathematical technique for validating the authenticity of digital document or message. This process is generated as a result of a sequence of operations: key generation, signing and verification algorithm. In the key generation, public and private keys are computed for the user. In the signing algorithm, sender signs the document with his private key. After signing, he attaches his signature to the document and sends it to the recipient. In the verification algorithm, recipient verifies the validity of the signature using the signature and the message together with sender's public key. A digital signature algorithm is called ‘unforgeable’ if any message/signature pair (m, s) not exists where s was not produced by the legitimate signer.

Merkle tree is a hash tree that contains hash values of data blocks and data blocks’ hashes hierarchically. In Merkle tree, every leaf node contains the hash value of a data block and every non-leaf node contains the hash value of child nodes. Trees are generated by hashing pairs of nodes until there is only one hash left, and this hash is called the root hash. It is the efficient and secure way to verify the contents of large data. Due to this feature, it is preferred in designing the blockchain applications.

Smart contract is a self-executing computer code running on top of a blockchain. It contains a set of rules to be executed and helps to exchange money, data or

anything of value. These contracts execute only when certain conditions are met. They reduce transaction costs by eliminating the third parties. Note that a smart contract can never be changed and no one can break the contract. Also it is distributed; the outcome of contract is verified by every node on the network.

Distributed ledger is a decentralized database system for recording transactions. Each node of the network can access the recordings and own an identical copy. Every changes or additions are reflected to each node's ledger. Periodically, nodes construct the transactions and update their copy through a consensus algorithm. Once the correct copy has been determined, all nodes update themselves with the correct copy of the ledger. Cryptographic hash functions and digital signatures are used to ensure the security.

Proof of work is a type of consensus algorithm that is used for confirming transactions and producing new blocks for the chain. When a new transaction is made, it must be validated and written to the block. To do this, users on the network try to solve a mathematical problem at a certain difficulty level. The user, who solves this problem, earns the right to write the next block to the chain. Note that the miners are rewarded with the certain amount of currency in order to be encouraged for mining.

3. Model

In this section, we explain our model and its core components that will be used to build our platform.

Our platform focuses on trading data collected from IoT devices in a safe environment. We utilize a number of primitives to realize our objective: blockchain for immutable and decentralized data storage; smart contracts for exchanging data and money authentically; digital signatures for providing authentication of users; and cryptographic hash functions for providing data integrity.

We design our platform as an open blockchain so that anyone can register the platform to commercialize his IoT data or to buy the IoT data sold in the platform. There are three different roles defined in our system, i.e. sellers, customers, and miners. A seller can advertise and sell his data through the platform by putting a brief information that describes the data, and a short proof that will be used to

prove the authenticity of the data. A customer checks the data advertised in the platform, and buys the data via a smart contract. A miner collects a certain number of available transactions in a certain period of time, and creates a block of these transactions through proof of work mechanism. Note that during the registration, the system generates a secret key-public key pair that will be used in the signature scheme deployed by the platform.

Our model can be viewed as two-phase protocol: uploading the data and executing the trade.

Uploading the data. In our model, the sellers do not keep their data in the blockchain. Instead, they use blockchain to market his data and to prove the integrity of the data. When a seller wants to commercialize his data through the platform, he prepares a small proof associated to the data using the technique proposed in [11].

Briefly, he divides the data into n small pieces $S_1, \dots, S_n$ of same length. Then he creates the Merkle tree of the data as shown in Figure 1. He then uploads the root R of the tree together with a brief information that describes the data. Note that the root of the tree R will be used to convince the customer that the integrity of the data will have been preserved during the marketing.

Executing the trade. Our platform enables the customers to check the quality of the data through a smart contract before buying it. When a customer wants buy some data advertised in platform, he first picks a random integer x from [1, n] as a challenge, and initiates a smart contract with the seller of the data.

The smart contract works as follows: for the challenge x, the seller sends the corresponding piece S_x to the customer. Note that, in our platform, it is assumed that any small piece of the data reflects the general structure of the data, and the quality and the usefulness of the data can easily be checked through this small piece. The customer then examines the sample. If the data satisfies the customer, he sends a confirmation (that can be just the integer 1 and 0 otherwise) to the seller. The seller prepares a proof π for the challenge x that consists of the siblings of the nodes on the path from S_x to the root in the Merkle tree of the data. Then it is checked through the smart contract whether the proof π is compatible with the root R uploaded in the platform.

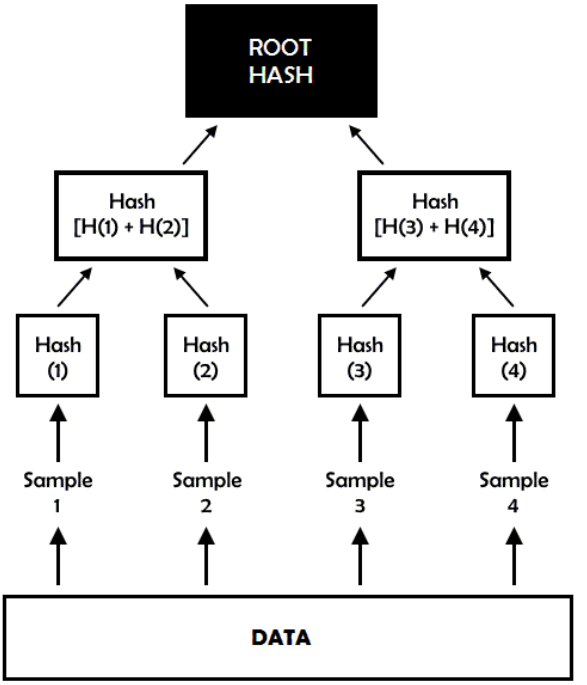

FIGURE 1. Generating Merkle tree from the data

For example, assume $n = 4$, $x = 2$, and the seller has created the Merkle tree of the data as in Figure 1. Then the proof π for the challenge the seller prepares will be $\pi = \left[H(S_1), H\left(H(S_3), H(S_3)\right)\right]$. It is checked whether

$$H\left(H\left(H(S_1), H(S_2)\right), H\left(H(S_3), H(S_4)\right)\right) \stackrel{?}{=} R. \tag{3.1}$$

If the proof is compatible with the root, the customer's money and seller's data are exchanged through the smart contract. Smart contracts allow us to protect both customers and sellers to incur losses in presence of any problems.

Figure 2 shows the basic operations in the smart contract for trading data and money, between sellers and customers. In a nutshell, the proof π of the challenge provided by the seller is compared with the root of the data already uploaded in the blockchain. Besides, it is also checked whether the customer has enough money or not. If one of them fails, the smart contract is terminated unsuccessfully and trade

operation is cancelled. Otherwise, the smart contract is terminated successfully and trade operation is completed.

All the transactions related to the trade are written to the blocks by the miners. Miners use the proof of work concept to establish a consensus for the current state of the ledger among all the entities in the network, i.e. miners collect the available valid transactions at the moment, calculate a proof of work for the new block consisting of the collected transactions, and add it to the valid chain. Miners get rewards corresponding to the effort they made by the system. Besides, a certain amount of fee for each transaction is paid to the miners in order to incentivize them for mining.

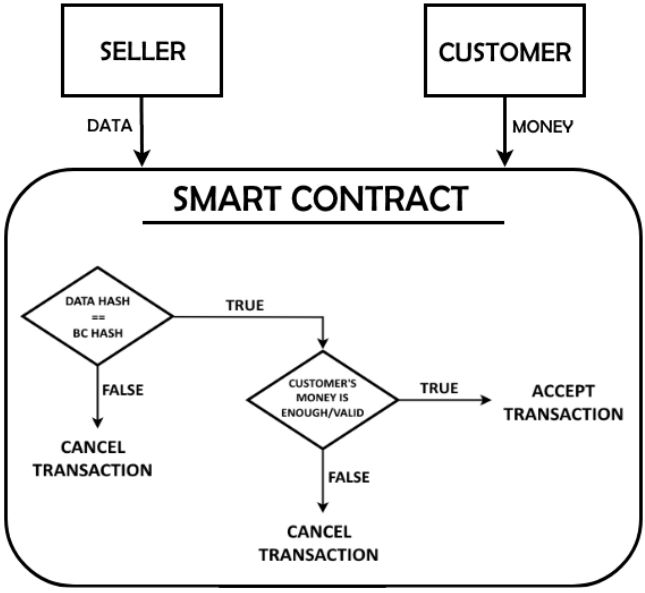

FIGURE. 2. Smart contract for trade operation.

4. Security analysis

This section provides a discussion on security and performance of our blockchain system and its structures.

As we stated before, when the customer requests sample from data, there is a possibility that the seller may send the wrong or useless sample. On the other hand,

the sample may belong to a useful data, but the data to be sent at the end may be an unusable data that is not relevant to the sample. Our platform solves this issue by having the sellers to put the root of the Merkle tree created on the data. Thus, the seller cannot make any change on the data after uploading this proof to the platform.

The users, who will trade among themselves, attach their signature to the transactions they create. The unforgeability of the digital signature scheme ensures that a user cannot impersonate any other users in the system. Also, no one in the system can alter the content of the transaction after it is deployed to the system.

Besides, any malevolent third party node can try to break or alter the transaction and message sequence in the chain. Due to the avalanche effect of the cryptographic hash function, block sequences and integrities can be checked fast and correctly. Even the slightest change in the block causes the hash value to change completely. Therefore, the consensus algorithm will not accept the manipulated block.

5. Conclusion

In this paper, we proposed an application for blockchain based IoT. It aims to market IoT data for money authentically. The system provides an immutable distributed database using blockchain. Besides, it provides confidence between the seller and the customer through smart contracts.

In our future work, we plan to implement this proposed system. We will also explore which file extension the IoT data should have.

References

[1] S. Haber, W.S. Stornetta, “How to time-stamp a digital document”, in Journal of Cryptology, vol. 3, no. 2, pp. 99-111, 1991.

[2] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, J. Wangasdad, “Untangling Blockchain: A Data Processing View of Blockchain Systems” in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, 2018.

[3] P. Ghuli, U. P. Kumar, R. Shettar, “A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices” in Advances in Computational Sciences and Technology, vol. 10, no. 8, pp. 2449-2456, 2017.

[4] I. C. Lin, T. C. Liao, "A Survey of Blockchain Security Issues and Challenges" in International Journal of Network Security, vol. 19, no. 5, pp. 653-659, 2017.
[5] "Watson IoT and Blockchain: Disruptor and game changer," https://public.dhe.ibm.com/common/ssi/ecm/ww/en/ww912350usen/watson-iot-cognitive-solutions-ww-infographic-general-ww912350usen-20180306.pdf
[6] S. Huh, S. Cho, S. Kim, "Managing IoT Devices using Blockchain Platform" in 19th International Conference on Advanced Communication Technology, 2017.
[7] S. Huckle, R. Bhattacharya, M. White, N. Beloff , "Internet of Things, Blockchain and Shared Economy Applications" in Procedia Computer Science, vol. 98, pp. 461-466, 2016.
[8] "Ambrosus - Enabling Sensors to Talk to Blockchain," https://ambrosus.com/.
[9] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy", arXiv preprint arXiv: 1712.02969, 2017.
[10] Elbuz, M. Osmanoglu, O. Tanriover, "Application of Blockchain Technology on Internet of Things" in 3rd International Conference on Theoretical and Applied Computer Science and Engineering (ICTACSE), Ankara, Turkey, 2018.
[11] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak. "Proof of Space", in Crypto 2015, 2015.

Current Address: Aydın ELBUZ: Ankara University, Computer Engineering Department, Ankara, Turkey
E-mail: aelbuz37@gmail.com,
Orcid ID: https://orcid.org/0000-0001-5932-8754
Current Address: Murat OSMANOGLU: Ankara University, Computer Engineering Department, Ankara, Turkey
E-mail: murat.osmanoglu@ankara.edu.tr,
Orcid ID: https://orcid.org/0000-0001-8693-141X
Current Address: Omer Ozgur TANRIOVER: Ankara University, Computer Engineering Department, Ankara, Turkey
E-mail: tanriover@ankara.edu.tr
Orcid ID: https://orcid.org/0000-0003-0833-3494