Decentralized M-Learning Platform with Trusted Execution Environment

Wennan Wang[1], Linkai Zhu[1,2(✉)], Baoping Wang[1], Li Guang[1], Sheng Peng[1,3], and Zhiming Cai[1]

[1] Institute of Data Science, City University of Macau, Macau, China
linkai@iscas.ac.cn
[2] Institute of Software Chinese Academy of Sciences, Beijing, China
[3] Zhuhai Yingying Technology Co., Ltd., Zhuhai, China

Abstract. With the rapid growth in E-learning, Mobile learning (M-learning) is one of the most widely used ways in distance education compare to the traditional classroom environment. However, Mobile learning has accentuated the problem of data privacy disclosure and low performance. Blockchain is an important step in smart contracts with peer execution, immutability, and provenance may bring a new level of protection and confidence to M-learning. In combination with Trusted Execution Environment, we proposed a decentralized M-learning platform prototype within TrustZone technology for ARM devices where the learner identity key is encrypted and stored in Hyperledger Fabric with a peer-to-peer network. Our platform resolves the difficulties with privacy data in E-learning and reduced workload. An evaluation demonstrated that It is available to execute encryption algorithms in a trusted execution environment.

Keywords: M-learning · E-learning · Blockchain · TrustZone · Privacy

1 Introduction

With the impact of the new coronavirus epidemic on normal teaching activities in colleges and universities [1], school teaching methods have changed to online methods in most countries. Online education platforms provide new solutions to ensure online teaching during the epidemic prevention and control period. School students can be free from space and learn online anytime, anywhere through the Internet.

With the development of wireless Internet technology and the widespread popularity of mobile devices. The software and hardware platforms of mobile devices run faster and more abundant applications [2]. People are also paying more and more attention to the advantages of mobile learning, focusing on creating a high-performance Mobile learning (M-learning) platform to better serve the majority of learners [3]. The equipment of M-learning includes an Android phone, iPhone, tablet, iPad, and notebook.

Intelligent push platform can solve the problem of content value judgment, but this is based on the user's privacy data exposure. The root cause of the problems encountered

W. Wang and L. Zhu—These authors contributed equally to this work.

W. Zhou and Y. Mu (Eds.): ICWL 2021, LNCS 13103, pp. 3–13, 2021.
https://doi.org/10.1007/978-3-030-90785-3_1

in the education industry is the lack of trust relationships and opaque mechanisms under the central network [1]. These devices collect and transmit large amount of privacy data in educational area when students or learners' study off campus using their smart phone [2]. Students' profile or personal data can be revealed through a centralized server. When M-learning personal data is opened for education, it is restricted by the permissions of the centralized server [3].

Blockchain has emerged as an interesting candidate because of its impressive features of decentralization [4]. By leveraging blockchain in the M-learning platform, the network efficiency of the single point server is improved since the growth of the number of learner nodes [5]. Blockchain can reduce the burden of the M-learning network with the number of connecting nodes is increasing [6]. And centralized M-learning system service often break data privacy policies by using data collected from learners for unauthorized purpose [7]. In order to address this issue in privacy related data between online education school and learners, we have designed and implemented a trusted decentralized M-learning platform prototype based on TrustZone device for Fabric Hyperledger. The privacy protection of each user's personal identity key need to be guaranteed through a trusted execution environment, and the decentralized access control system of the blockchain.

However, most blockchain-based platforms use digital pseudonyms [8], allowing users to have multiple pseudonyms, but this approach only provides weaker user identity anonymity [9], the correlation between transactions, and the student or learner's information are exposed on the blockchain, and all public key addresses of a E-learning learner may be inferred if one of the user's addresses is compromised.

Since TrustZone is the domain of trusted computing in the ARM architecture. Such devices like mobile phones and tablets provide a common execution environment (Rich Execution Environment, REE), which will run Android, IOS and other intelligent operating systems in this environment to provide users with a variety of services [10]. Based on the trusted execution environment provided by the ARM TrustZone architecture, this paper analyzes the definition of the trusted platform module TPM specification, and designs its Kernel functions, including integrity measurement, key generation and management, and symmetric asymmetric encryption and decryption. This provides basic security support for trusted services such as trusted startup of upper-level applications and components of the M-learning platform and blockchain network connection, thereby improving the security of students using mobile smart terminals.

In this work we leverage blockchain to reduce the load of network and improve the performance of M-learning platform. We provide a method for secure identity key by trusted execution environment. We have implemented a Trusted M-learning platform prototype on blockchain using Hyperledger Fabric.

The paper is structured as follows. In Sect. 2 we provide technologies on E-learning, M-learning, Blockchain, and TrustZone. In Sect. 3 we discuss the overview of the architecture. In Sect. 4 we describe how we design and implement the decentralized M-learning platform. In Sect. 5 we provide evaluation of the approach. Finally, Sect. 6 we conclude the paper.

2 Technologies

E-Learning
E-Learning often used in online education, also known as electronic learning. It is a way to use Internet technology to disseminate learning resources and quickly learn. It is one of the main ways people acquire knowledge. People can learn online through the Internet, which broadens people's learning channels and improves Learning efficiency, better use of fragmented time for learning. The E-Learning platform has a large amount of behavior data left by user learning, which can more accurately match the learning needs of users after mining and analysis.

M-Learning
M-learning as Mobile Learning, the adoption of Mobile Learning can provide stimulating new possibilities for students, teachers, and school staff through new forms of training and learning innovations [11].

Blockchain
Blockchain, mainly known as the technology for operating Bitcoin encrypted currency [12], is a kind of multi-party participation and joint maintenance of a distributed database. It is based on a peer-to-peer network and uses encryption algorithms and digital signatures in cryptography to ensure the data itself Integrity and immutability and security of access. It uses chain data structure to verify and store data for building the overall structure of blockchain through consensus mechanism. And this kind of distributed accounting has gradually become one of the Internet applications in recent years. An important function. It maintains an ever-growing data block. The data recorded in each block cannot be tampered with or modified. Since there is no central node, all participating nodes can store data. Its decentralized nature provides a viable solution to build security protocols without the need for a third party (Fig. 1).

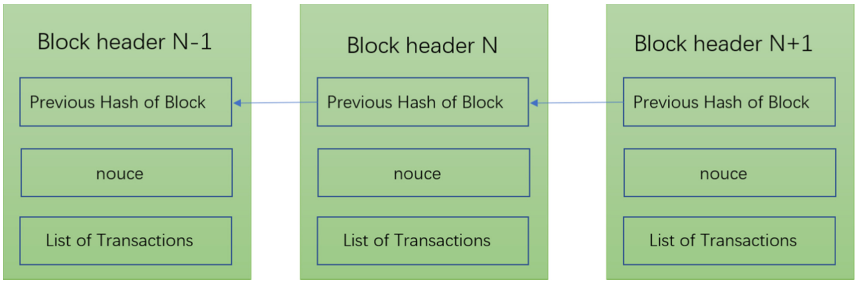

Fig. 1. Blockchain structure

Trusted Execution Environment
The trusted execution environment (Trusted Execution Environment, TEE) provides a completely isolated environment in the CPU, called a safe zone, which can prevent

other applications, operating systems, and host owners from tampering to ensure that the code is executed in the TEE. And Data and stars and integrity are protected [13]. Even understand the status of applications running in the safe zone. By using both hardware and software to protect data and code, TEE is more secure than operating systems. We leverage TEE to enhance blockchain performance, efficiency, and security.

TrustZone

ARM proposed a hardware-level mobile platform security technology called TrustZone [14]. The basic principle of TrustZone technology is to virtualize a physical Kernel into multiple Kernels, and use monitors to switch different states, thereby constructing a processor security environment. This technology uses the increased security features in the CPU to cooperate with software and hardware to construct a Trusted execution environment (TEE) completely isolated from ordinary execution environment (REE).

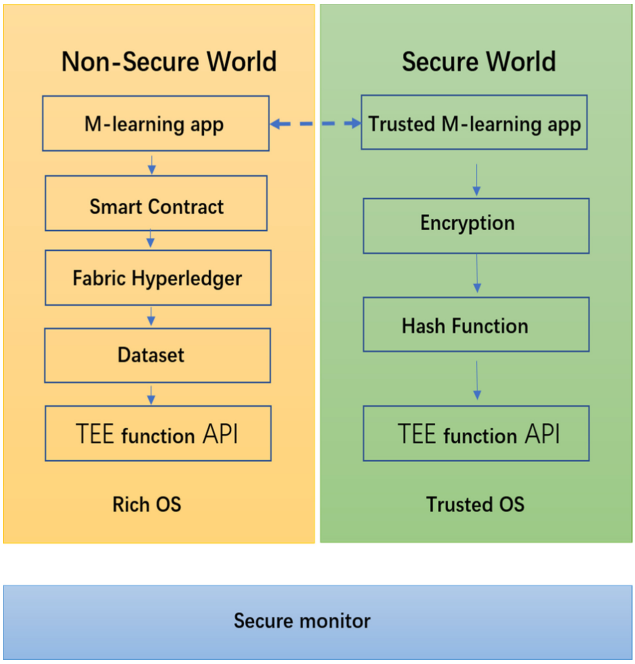

Fig. 2. M-learning TrustZone architecture

The blockchain can store data and perform computation on every decentralized learner all around the world and the hashes of transactions generated from E-learning devices [15]. Fabric Hyperledger is chosen as a local blockchain architecture, which is an open-source fundamental technology WW [16]. For prototyping, the data of M-learning is collected from different learning apps. For each communication between devices or nodes, a transaction is created and stored in the blockchain. As shown in Fig. 2, the ARM TrustZone-enabled application is composed of secure and non-secure world. In secure world, the sensitive operations are called (encryption and hashing).

3 Overview

The proposed M-learning platform consists of three main components which includes arm device client, TrustZone module and blockchain.

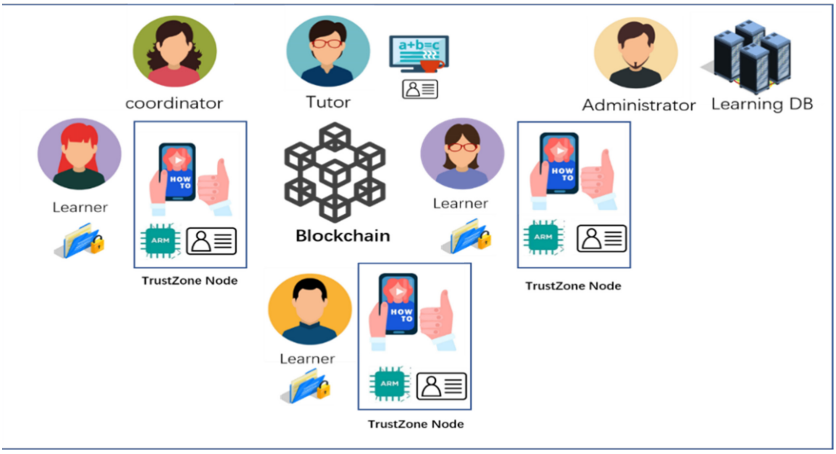

Fig. 3. Decentralized M-learning platform with TEE

All these components are going to solving the problem:

Security of M-Learning Platform with Blockchain
The decentralized and distributed nature of blockchain makes it a promising solution for M-learning security. Mobile phone as a new E-learning device with integration in blockchain enables a higher security level.

Scope and Assumption
The scope of this paper considers the decentralization of data access management using blockchain and data protection using TrustZone. We designed and implemented a security M-learning course platform where user have equal right in managing their data. For this platform, the private data is supposed to encrypted by using asymmetric cryptographic protocols. In this paper we do not consider phishing attacks and denial of service attacks.

Trusted Blockchain M-Learning Platform Components
As shown in Fig. 3, several components are composing the proposed Trust chain M-learning platform:

- Tutor/teacher, the role is to create and upload lessons, after uploading it, this role will release to learners.
- Learner: The learner can register account and download released lessons from tutor. Students can input the course notes in database.

- Coordinator: the role is to disseminate the information to colleagues within the department. Obtain updates and alerts form E-learning group.
- Administrator: Administrator is to manage the E-learning course data and maintain the platform
- Learning Resource Database: The E-learning database is to store E-learning resources include learner's information (course, scores, and records).
- Blockchain: store the hash of the encrypted identity data in the blockchain.
- TrustZone node: the process of encryption is executed in TrustZone.

Trusted Identity Key

M-learning identity key management lacks effective management technology, and key leakage and loss caused by improper use and storage will bring losses to users, and no central node participation in the blockchain will make key management difficult. Using under-chain TrustZone to store wallet-like methods, in an isolated state, the key wallet is executed in this environment to prevent malicious soft attacks and theft of user keys.

Since Fabric Hyperledger is an open-source smart contract platform, the above support can only be contract is public, usually involves multi-user participation, user account information, transactions and status information are exposed in the network, the need to increase privacy protection mechanisms, because most E-learning users are now popular use of smart devices, through arm architecture-based TrustZone to enhance smart contract privacy protection, build a trusted execution environment.

In a processor architecture, each physical processor Kernel provides two virtual Kernels, one non-secure and the other secure Kernels. The mechanism for switching between the two Kernels is called the monitor mode. The non-secure Kernel can only access non-secure system resources, while secure kernel energy accesses all resources. Software in the ordinary world can use Secure Monitor Call (SMC) instructions or through a subset of hardware exception mechanisms to enter monitor mode.

When the user mode of the normal world needs to obtain the services of the secure world, first need to enter the privileged mode of the normal world, call SMC in this mode, the processor will enter the secure monitor mode, monitor mode back up the context of the normal world, and then enter the privileged mode of the secure world, at this time the operating environment is the execution environment of the secure world, and then enter the user mode of the secure world, perform the corresponding security services (Fig. 4).

Decentralized M-Learning Platform Architecture

M-learning is based on the trusted blockchain. The M-learning device indicates that the learner login the M-learning node, and the node number is unique. After students log on, the profile data interacts with user management through the web service interface, while the identification number is verified with the data accessed by the student. The data communicates between the institution and the student. Identity numbers are encrypted using asymmetric encryption algorithms in TrustZone through smart contracts, encrypted identity keys are stored in the blockchain through smart contracts. M-learning users can access their profile data without leaking it since identity key is perform encryption

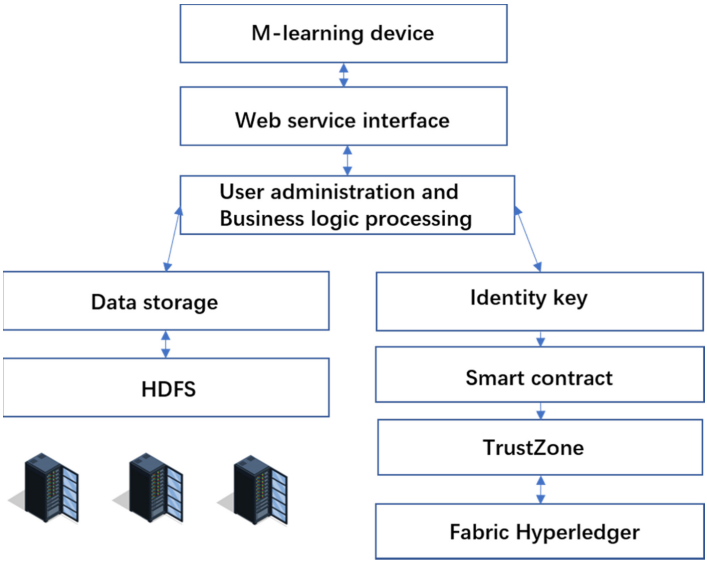

Fig. 4. Decentralized M-learning platform data flow

operations in an isolated environment. This idea adapts to a broader E-learning style and goals. Connections to any new E-learning node are authenticated by blockchain network.

4 Implementation

We used six real processor based on the arm architecture of the smart phone to implement M-learning platform using the Fabric Hyperledger which is a distributed ledger with blockchain as the underlying. The M-Learning platform including the course search engine system and access control management platform, as well as the recommendation module.

Smart Contract Process
Blockchain guarantees that the intra-chain computing process is credible through smart contracts and consensus mechanisms. Here the smart contract is essentially a programmable state machine, and in most blockchains, block time is fixed. It takes to process the business and the latency of M-Learning's network. The solution needs to keep M-learning's business processes out of the blockchain and handle only the state of business initialization and the final state on the chain. This is done by separating business logic from consensus logic and moving the computing portion of performance consumption down the chain for privacy and performance savings.

Data Storage
The data storage layer is mainly responsible for storing and storing the course data generated and collected during the operation of other layers. The system in this paper mainly uses HDFS and MySQL, in which MySQL stores the course information of users,

as well as the structured data of users' historical behavior, such as rating and collection. HDFS is used to store course courseware video resources and other unstructured data.

Web Browser

The web interface is the interactive interface between users and the system, which provides learners with the basic operating functions of the online education platform and supports personalized course recommendation. The browser presents the response results to the user. This layer also generates user behavior data, which can be used by other layers for calculation and analysis (Figs. 5 and 6).

Fig. 5. Trustzone node in fabric hyperledger

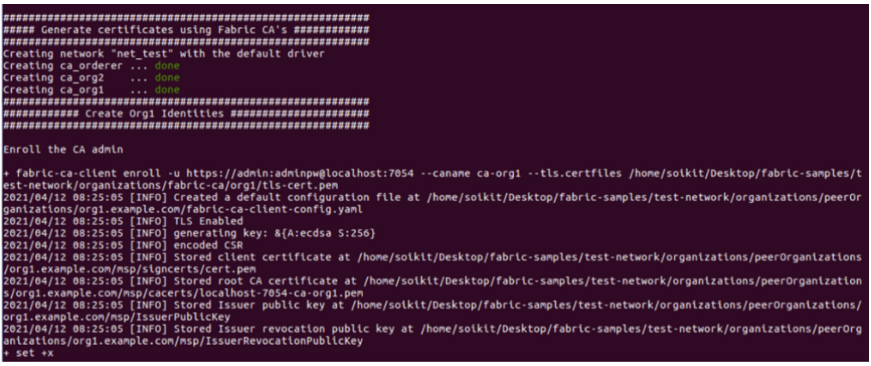

Fig. 6. Identity key setup process

Create Identity Key

When the user logs in, the blockchain system will decide whether he or she is a registered user of the platform. The registered user can enter the homepage of the course recommendation system after entering the corresponding user name, password, and verification code. Unregistered users will jump to the registration interface, fill in the registration information, and then log in as registered users (Figs. 7, 8, 9 and 10).

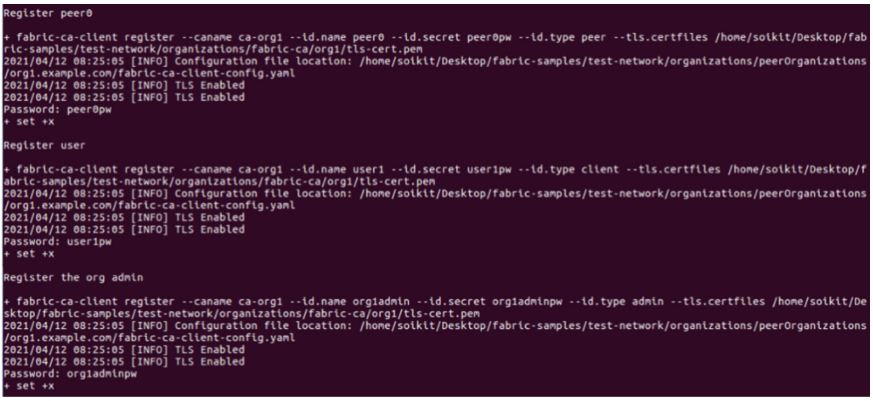

Fig. 7. M-learning role registration

Fig. 8. Educational service frontend user interface

Fig. 9. Student frontend user interface

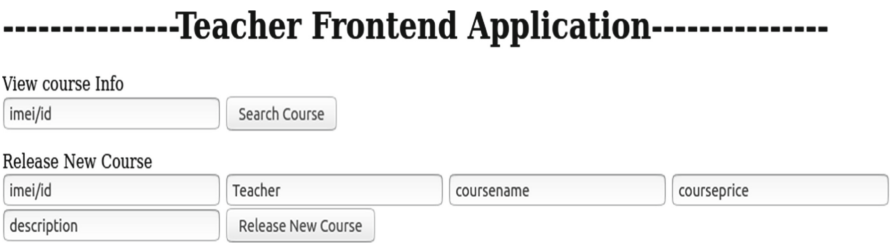

Fig. 10. Teacher frontend user interface

5 Evaluation

In Fig. 11, it shows the impact of the transaction workload execution on the blockchain. When encryption operations are performed in TrustZone, the write workload is slightly higher than without using TEE. The cryptographic algorithm is performed in an isolated environment when measuring the transaction throughput of the M-learning node. When it is at 600 write workloads, the transaction throughput is 11.17 writes per second. As the write workload increases to 2000, the write throughput stabilizes at 7.82 writes per second. Instead of executing a cryptographic algorithm in an isolated TrustZone, the transaction throughput is 6.24 writes per second at 600 write workloads. At 2000 write workload, transaction throughput drops to 5.61 writes per second.

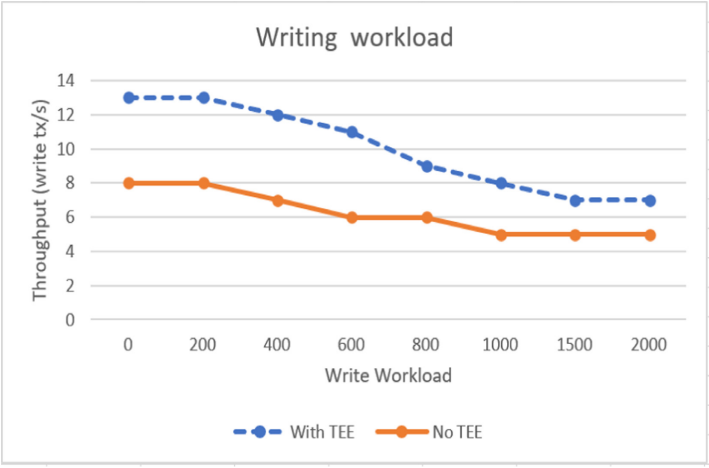

Fig. 11. Throughput and write workload

6 Conclusion

In this research, it introduces M-learning platform in many decentralized nodes that leverage a decentralized network of peers accompanied by a public ledger. However, in terms of blockchain, it encounters some privacy threats, which limit its realistic applications. we have presented a solution that utilizes the combination of TEE and Hyperledger Fabric in M-learning platform. Particularly, for securing identity key, an asymmetric encryption algorithm is used in TrustZone secure world for realizing blockchain privacy demands. Besides, our approach utilizes blockchain to reduce workload. An evaluation revealed that the throughput of our approach is tend to be stable for encryption of the identity key in a trustworthy execution environment, which means, this method protects the user's personal privacy without compromising performance.

Acknowledgments. This research is supported by the: 1. project funded by Zhuhai Industry-University-Research Cooperation Project: Research on Key Technologies of Cross-domain Data

Compliance and Mutual Trust Computing in Zhuhai and Macau (No. ZH22017002200011PWC) 2. Research on knowledge-oriented probabilistic graphical model theory based on multi-source data (FDCT- NSFC Projects: 0066/2019/AFJ) 3. Research and Application of Cooperative Multi-Agent Platform for Zhuhai-Macao Manufacturing Service (0058/2019/AMJ).

References

1. Rodrigues, H., Almeida, F., Figueiredo, V., Lopes, S.L.: Tracking e-learning through published papers: a systematic review. Comput. Educ. **136**, 87–98 (2019)
2. Anwar, M.M., Greer, J., Brooks, C.A.: Privacy enhanced personalization in e-learning, p. 1 (2006). https://doi.org/10.1145/1501434.1501485
3. Zhao, W., Liu, K., Ma, K.: Design of student capability evaluation system merging blockchain technology. J. Phys. Conf. Ser. **1168**, 032123 (2019)
4. Bernabe, J.B., Canovas, J.L., Hernandez-Ramos, J.L., Moreno, R.T., Skarmeta, A.: Privacy-preserving solutions for blockchain: review and challenges. IEEE Access **7**, 164908–164940 (2019)
5. Lam, T.Y., Dongol, B.: A blockchain-enabled e-learning platform. Interact. Learn. Environ. 1–23 (2020)
6. Masud, M.A.H., Huang, X., Islam, M.R.: A novel approach for the security remedial in a cloud-based E-learning network. J. Netw. **9**, 2934 (2014)
7. Anwar, M.: Supporting privacy, trust, and personalization in online learning. Int. J. Artif. Intell. Educ. (2020). https://doi.org/10.1007/s40593-020-00216-0
8. Peng, L., et al.: Privacy preservation in permissionless blockchain: a survey. Digit. Commun. Netw. **7**(3), 295–307 (2020). https://doi.org/10.1016/j.dcan.2020.05.008
9. Zhu, X., Badr, Y.: Identity management systems for the Internet of Things: a survey towards blockchain solutions. Sensors **18**, 1–18 (2018)
10. Muller, C.: Execution of smart contracts with ARM TrustZone, p. 45 (2019)
11. Oakes, K., Green, D.: E-learning. T D, vol. 57, 17–19 October 2003
12. Nakamoto, S.: A peer-to-peer electronic cash system (2008)
13. Van Schaik, S., Kwong, A., Genkin, D., Yarom, Y.: SGAxe: How SGX Fails in Practice (2020). https://Cacheoutattack.Com/
14. Ali, J., Ali, T., Alsaawy, Y., Khalid, A.S., Musa, S.: Blockchain-based smart-IoT trust zone measurement architecture. In: ACM International Conference Proceeding Series, Part F1481, pp. 152–157 (2019)
15. Ubaka-Okoye, M.N., et al.: Blockchain framework for securing e-learning system. Int. J. Adv. Trends Comput. Sci. Eng. **9**, 2933–2940 (2020)
16. Wang, S., Zhang, Y., Zhang, Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access **6**, 38437–38450 (2018)