A Blockchain Based Digital Certification Platform: CertiDApp

Kerem Ataşen
Department of Software Engineering
Kırklareli University
Kırklareli, Turkey
atasenkerem@klu.edu.tr

Bora Aslan
(Corresponding author)
Department of Software Engineering
Kırklareli University
Kirklareli, Turkey
bora.aslan@klu.edu.tr

***Abstract*— Nowadays, a diploma or certificate is required for any kind of application; for application to a higher level of education, a job application or a scholarship application. When submitting these documents to the requesting party, they agree that they will declare the accuracy of the documents they submit and that they will be the direct interlocutor of the criminal proceedings in case of document fraud. Universities and other educational institutions have started to add QR codes to their certificates in order to prevent forgery of documents. According to plans, the accuracy of the documents can be confirmed by the requesting institution through the QR code. However, since this confirmation will be made from a central database, proof of unmodified data or real documents cannot be presented to the diploma requesting party. Because centralized data storage systems are vulnerable to any kind of malfunction. In this study, a solution is suggested with a decentralized application (DApp) that runs on blockchain that communicates with smart contracts.**

Keywords—Blockchain, Smart Contracts, DApp, Solidity, Ethereum

I. Introduction

Today, a diploma, certificate or a certificate of competence and knowledge is required for any application, whether for application to a higher level of education, for a job application or for a scholarship application. The educational institution where the diploma is received serves as a third party between the holder of the diploma and the party requesting the diploma. The possibility that any changes have been made in the process from the issuing institution to the requesting institution undermines the reliability of the process. An employee of the institution issuing the document may intervene in the same way as the contents of the document. It is also possible that such a document may not exist at all. The person can prepare a document in digital environment and deliver it to the requesting institution as if it really deserves it. As a solution to such malicious situations, some institutions submit documents containing QR codes to people and question the accuracy of the data by reading these QR codes. However, the fact that the data is stored centrally is ignored. As long as this situation continues, all other solutions will be meaningless. The classical database services used by this monopolized system in general do not provide a service to confirm the correct version of the document in a possible intervention. Even if data is backed up, the number of backups will not be large, considering the cost, and this is not a very healthy solution. Based on this it can be concluded that the more information is the same in more places, the more accurate it is.

In this study, a blockchain based digital certification application has been developed as a solution to the shortcomings of classical database system based applications. Institutions that provide documents such as diplomas or certificates will enter personal information, graduation information and upload the diploma document of people to the system as a PDF file. Document uploading to the system will be performed by the persons designated and authorized by the institution. After the information is uploaded to the system, a hash value will be given to the person and this hash value will be used for the verification of the document by the requesting institution. The application has a separate interface for the people or institutions that will perform the verification process.

II. Methods and Technologies

A Truffle box was used as a DApp template. The necessary web pages for the interfaces were created and the smart contract with the Solidity language was written in a .sol file.

The balance of one of the test accounts in the Ganache application was transferred to an Infura node via Metamask as a test balance via private key.

A. *Blockchain*

The blockchain technology, which first appeared in 2008 by Satoshi Nakamoto's article “Bitcoin: A Peer-to-Peer Cash System, started to be offered as solution suggestion in digital identification, copyright and patent ownership, finance, banking, health care, education and supply chain, that require confidence guarantee, high traceability, data security and transparency [1].

From the past to the present, third parties have emerged as a security guarantor due to the fact that people who are communicating or consciously shopping for any reason do not trust each other. Blockchain is a distributed ledger technology in which the transactions that are required to be kept in record are encrypted and stored in structures. The first block in the blockchain is called Genesis block. Each block after the Genesis block has the encrypted information of the preceding block. Thanks to the encrypted information of the previous block in each block, the ancestor blocks in the blockchain can be accessed retrospectively from child blocks [2]. Blockchain is not an ordinary recording system like classical or distributed database systems, SQL Server, MySQL, Jena, Neo4j or InfluxDB. Because it do not allow any update or delete processes in contrast of classical recording systems. In addition, all transactions recorded in the blockchain contain a timestamp. This is a crucial feature for reliability, demonstrability and verifiable. More importantly, if any changes occur in a block of blockchain, any other blocks that comes after mutated block will be changed and invalid. However, in database systems that is not occur, only mutated data changes and other data remains same and valid.

In blockchain networks, there is a collection of nodes as participant. Appending a new block to the blockchain is only could be done by reaching consensus. If a consensus is reached, that means a new block could be added by a node. These processes are controlled by some consensus algorithms, such as Proof-of-Work [1] or Proof-of-Stake [7]. In CertiDApp case, an Ethereum based blockchain test network is used. Current version of Ethereum uses the Proof-of-Work algorithm to reach consensus.

B. Smart Contracts and DApp

When the idea of smart contracts appeared towards the end of the 1990s, it was defined as digital contracts which operate when the necessary conditions are occur like classical contracts [3]. According to Christidis and Devetsikiotis, smart contracts can be expressed as digital programs based on a platform-specific blockchain consensus protocol, which will be executed automatically when the terms of the agreement are fulfilled and self-implemented due to its decentralized structure, without intermediaries and protected against interference [4]. It is not possible to run smart contracts on every blockchain platform. Blockchain platforms like Ethereum, Stellar, NEM, Hyperledger Fabric, Snax, Tezos, Waves, Neblio and Lisk are platforms that can store and run smart contracts. In this study, Ethereum platform which is the most known of these platforms was used. According to Ethereum yellow paper, a special creation process is executed to introduce smart contract to the blockchain. At the end of this process, a unique contract account is created, which is assigned a unique 160-bit address. After the successfully completion of that introducer transaction, the code of the contract was loaded into the blockchain. From now on, it is not possible to intervene in this unique addressed smart contract [5]. Other Ethereum contract or wallet accounts can then send transactions and interact with them using unique addresses assigned to the contracts. Smart contracts can be programmed in different programming languages depending on the blockchain platform they run. In this study, Solidity programming language, which was created for writing smart contracts on Ethereum platform, was used. In addition, programming languages such as Serpent, Vyper, Plutus, QSCL and Marlowe have been developed for different platforms.

Unlike today's centralized Web or mobile applications (CAPP), DApps are transparent, traceable, flexible and better incentive anti-centralized applications that do not run on a central server or machine. The information about the application is also not stored in a central database. [6]. Data is stored in blockchain or decentralized storage solutions like Storj and IPFS. Due to the decentralized operation of the DApps in the blockchain network and the data being distributed in the blockchain, the crashing of any machine in the blockchain network will not make the application and data inaccessible. Because same data and application will be existed in any blockchain member and accessed from any members of blockchain network. The working logic of DApp and classical applications is given in Figure 1.

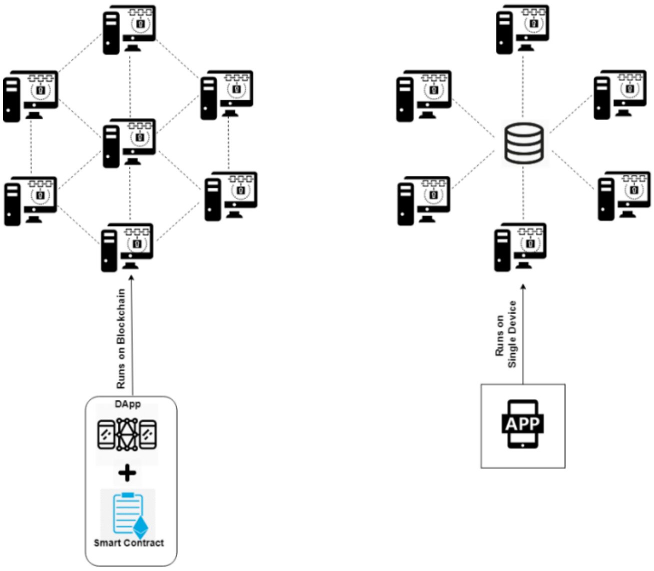

Fig. 1. DApp and CApp Working Logic

C. Truffle, Ganache, Metamask and Infura

Truffle is a service that provides DApp templates with smart contracts called box [7]. It can be thought as Web's Wordpress. In this study, a box was downloaded from Truffle website and it was edited according to use case. These processes were performed in Node.js command line. After any other necessary operations has done, DApp will be live in by default http://localhost:3000.

Ganache is a service that provides a special blockchain and transaction history simulation on local computers [8]. The number of blocks, mining time, and hash information can be accessed through the interface. Initially it has 10 different accounts that include 100 ether (the main cryptocurrency unit on Ethereum network) test balance.

When developing this application, it is necessary to transfer the balance of the Ganache test accounts to a test account to fund the fees of the tests to be performed. For this purpose Metamask browser extension is used. Metamask is an extension that allows non-hardware-enabled machines to receive this service through a browser [9]. With this extension, the Infura infrastructure, which provides a blockchain test network, is used, including an account to which the test balance is transferred [10]. The operation flow of the CertiDApp is shown in Figure 2.

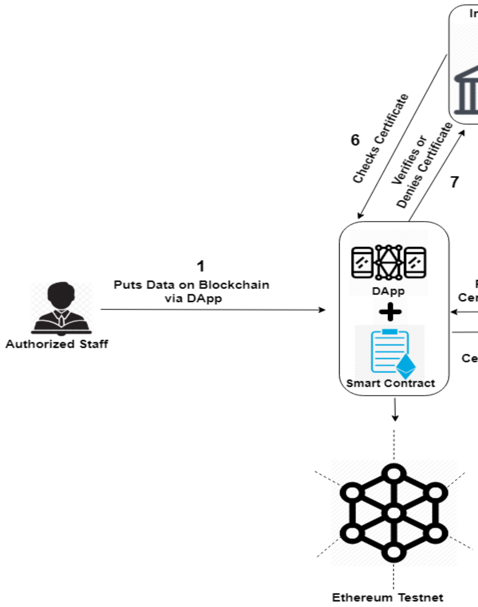

Fig. 2. CertiDApp Operation Flow

III. Operation Flow in Depth

The operation flow of CertiDApp platform can be divided into seven ordinal different works. These different works are numbered as seen in Figure 2 above. In first step, an authorized staff uses the CertiDApp platform to put certificate document and any other necessary information data on blockchain by using a web interface. The authorized staff might be a member of the authority to issue certificates. It is assumed that staff is a trusted stakeholder of that system. There is no doubt on him and his works. After this work, data provided by authorized staff is stored on blockchain. In second step, the other stakeholder, student which is issued with a certificate from an authority, queries the CertiDApp to fetch his or her certificate data. CertiDApp gives response to student with the exactly requested data. In next step in that operation flow, step 4, a company asks for a certificate from the applier, in this case the applier is a student which is graduated from that authority. As a response for this request, applier gives the requester the certificate at step 5. The other steps, 6 and 7, requester asks CertiDApp for validity of the certificate which provided by the applier. CertiDApp looks for the questioned certificate to the blockchain. If a match exists then it validates the certificate.

Appending a new certificate and the other information about the student to the blockchain, questioning validity of information provided by applier from that blockchain is controlled by a smart contract that written in Solidity language.

IV. Evaluation and Conclusion

Centralized data storage in classical systems leads to the questioning of trust in data. This is because data stored on a central server or a distributed database is always vulnerable. In case of any attacks, data cannot be recovered. The institutions that provide security guarantee are trying to solve these problems. Nevertheless, getting services from these institutions means increasing costs. Even in this case, the trust in the data remains controversial. Because, data is still in a centralized institutions databases. With the development of the block chain technology that comes to our attention as a solution to these deficiencies, it is seen that decentralized applications and smart contracts are gaining importance in terms of trust in data.

A DAPP has been developed that includes smart contracting with the Solidity programming language, which is unquestionably secure than classical central applications. All data about this DApp is stored on blockchain. By this way, application and data will not be centralized anymore, they will more secure and reliable. With the developed DAPP, the educational institutions issuing the certificates of the students graduated from universities will be able to keep their certificates in a block chain that cannot be changed, tracked backwards and in a transparent way. Employers will be able to check the accuracy of the diplomas presented to them by graduating applicants from the blockchain through the developed DAPP. Since the diploma data is saved in a blockchain and not in a central database, no intervention is possible. This prevents fake, invalid or never-existed diplomas being as if exist. In blockchain, storing the chain in all network members brings data reliability and security. Storing same data on every member node brings a bad result, scalability of blockchain. This developed DApp will prevent unfair gains or promotions that originated from diploma and certificate fraud. Also no data were used to support this study.

V. Future Works

Decentralized storage solutions IPFS and Storj can be used to store data as a solution to the scalability problem. For other centrally controllable documents such as identity, driver's license, marital status, etc., this DApp can be made available with some fixes. In addition to the Ethereum platform, CertiDApp smart contracts might be written in other smart contract languages. Therefore, CertiDApp will be run on other smart-contract-runner blockchain platforms.

References

[1] Pilkington, M. (2016). 11 Blockchain technology: principles and applications. Research handbook on digital transformations, 225.

[2] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

[3] Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9).

[4] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

[5] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151, 1-32.

[6] Raval, S. (2016). Decentralized applications: harnessing Bitcoin's blockchain technology. " O'Reilly Media, Inc.".

[7] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19.

[8] https://truffleframework.com/boxes

[9] https://truffleframework.com/docs

[10] https://metamask.io/

[11] https://infura.io/