Document Verification using Blockchain for Trusted CV Information

Conference Paper · July 2020

CITATIONS
7

READS
3,472

2 authors, including:

Venkata Marella
Aalto University
8 PUBLICATIONS **61** CITATIONS

SEE PROFILE

Aug 10th, 12:00 AM

Document Verification using Blockchain for Trusted CV Information

Venkata Marella
Aalto University, venkata.marella@aalto.fi

Anoop Vijayan
Tuxera Inc, anoop@tuxera.com

Document Verification using Blockchain for Trusted CV Information

Completed Research

Venkata Marella
Aalto University
venkata.marella@aalto.fi

Anoop Vijayan
Tuxera Inc
anoop@tuxera.com

Abstract

With the changing landscape of the job market, it is very difficult to secure a job in a company. People manipulate their curriculum vitae with fake information to find a job. Multinational National Companies are investing heavily to verify the background details of the job applicants. But, the background verification process implemented by these companies is extremely costly, time-consuming, and inefficient. To resolve this problem, we present a working prototype of a solution using Design Science Research Methodology where the hash values of all the original documents of a job applicant provided by various organizations are saved on a consortium blockchain. The job applicant's details can be verified during the hiring process by comparing the hash value of the given document with the hash value of the document present on the blockchain. This process is extremely efficient, less time-consuming, and very cheap to implement for all kinds of companies.

Keywords

Blockchain, Hash Value, Background Verification process, and Design Science Research Methodology.

Introduction

In today's competitive world, finding a job is not an easy task. So, people are likely to lie on their Curriculum Vitae (CV) when applying for jobs (O'Donnell, 2017). A candidate may lie about his/her educational background, work experience, skillset, grades, criminal record, etc. According to the Signaling theory, two parties may not share accurate information if they have partly conflicting interests (Bangerter et al., 2012). The job applicant's interest is to secure a job that offers a good salary, while the employer's interest is to hire the candidate with the required skills that the job demands. In such a situation, there is no guarantee that the job applicant would share accurate information with the employer. Hiring decisions based on such sort of false information can be catastrophic for any organization. Even the information posted on social networking sites like Linkedin can't be trusted (Brown, 2017). According to the survey conducted by CareerBuilder, around 56% of the hiring managers caught applicants lying on their resume and 62% of the people tried to embellish their skills or capabilities for a job interview (White, 2015). In England, according to the UK Higher Education Degree Datacheck (HEDD) survey around 33% of the job applicants put false information on their CV and 40% of them falsified their academic qualifications, while 11% of them made up a new degree all together (Campbell, 2015). In South Africa, around 16% of the job applicants lied on their resume. The survey found out that an increasing rate of unemployment is one of the reasons for the job applicants to lie on their resume (Ina van der Merwe, 2015). In India, a survey conducted by a background verification firm confirmed that 50% of the job applicants forged their previous job experience certificates. In some employment sectors, the number of such forged qualifications is as high as 71.5% (Shukla, 2014). Educational details are of crucial importance in the hiring process. Certain studies suggest that 30% of the job applicants falsify information related to degrees received, institutions attended, or professional memberships (Buckhoff, 2003; Rosen, 2007; Jund-Ming, 2000). Job Applicant can exaggerate his work experience to convince the employer that he/she is capable of the position.

The hiring process has become a daunting task for the human resource departments of organizations due to the false information provided by the job applicants on their CVs. In India, companies hire some third

party agencies to do background verification of all the newly hired employees and spend a lot of money on this process. There are some strict laws against using a fake resume in countries like Australia (Kraps, 2015). In Western Australia, local government regulations gave the authority to the state government to impose a $5000 fine on all the job applicants for CEO positions who try to produce fake information on their curriculum vitae (Office, 2013).

There could be several reasons why a job applicant would lie on his CV. It could be long-term unemployment, a desire for high pay, or high competition for jobs in the country. People lie on their CV for all kinds of job positions including the CEO and CFO positions. In such an environment, it is very difficult for HR departments of the organizations to find people with the required skill set for the job. HR departments of various organizations spend a lot of money to verify the background details of potential candidates for a job position. Hence, finding a candidate with the required qualification for a job is a challenge for any organization in many countries. Therefore, our research question is as follows.

"*How to authenticate the information on the CV provided by a job applicant immediately at a low cost?*"

We offer a solution using blockchain to provide the organizations with trusted information about the job applicant's background details during the hiring process. In the next sections, we will discuss the current process of CV verification. In the following sections, we will talk about the technical concepts of Blockchain technology and cryptographic hash. Then, we will talk about our research methodology and propose our solution. We will elaborate on our solution with a workflow diagram and conclude the paper with the advantages of our proposed solution.

Current Process

Whenever a job applicant applies for a job, the information on his CV is not verified immediately. It is only when the job applicant clears the interview, the company asks the job applicant to submit copies of his original documents like the University transcripts, work experience, criminal records, and other certification documents (Bonanni et al, 2011). Usually, companies verify these documents either by emailing, telephoning, or physically going to the concerned organization and verifying the authenticity of the documents. In the current globalized world, companies do need to hire employees from various countries. The process becomes much more difficult when the job applicant is from a different country. But, very few Small and Medium Enterprises (SMEs) verify these documents. It would cost money, time, and resources for them to verify these documents, which they cannot afford. The company needs to hire more human resource staff or pay a third-party agency to verify the background of the selected job applicants. It takes several days for them to finish the process and it can delay the hiring process. Sometimes, there could be some errors or manipulations in the background verification process and it might fail to identify the false information provided by the job applicant. But, many studies suggest that the background screening process would reduce the theft, and improve the organizational performance (Jund-Ming, 2000; Keller, 2006). For the companies that don't verify the information on the CVs, it will take several months for them to assess the performance of the employee and figure out that he lied on the CV. During this process, the company will have paid several months of salary and invested a lot of time and resources on the person. The costs incurred due to bad hire are generally estimated to be at least double the employee's annual compensation through costs such as lower productivity and lost customers through poor service (Jund-Ming, 2000). Hence, the hiring process without involving the background verification process will be catastrophic for the company.

The current process of hiring and verifying the background details of the job applicants can differ from one company to others and sometimes it also depends on the laws of the country where the company is located. Regardless of the company or the country, the process of verifying the information provided by the job applicants on their CVs is a tedious task involving money, time, and resources.

Blockchain Technology

Blockchain Technology is a decentralized and distributed database where all the transactions are recorded in a ledger (Glaser et al., 2014). Blockchain stores the information across a network of personal computers

that are globally distributed called nodes. These nodes are connected by a Peer to Peer (P2P) communication protocol with a layer for node communication and peer discovery (Glaser et al., 2014). There is no centralized authority that owns the access to information. Every node in the network can access the information and process the transactions. One node in the system cannot manipulate the data because all the other nodes have access to correct information. Hence, the data stored on the blockchain is extremely secure. Transactions are bundled into blocks and each block references the previous block of transactions, thereby achieving a temporal sequencing of transactions (Narayanan et al., 2016). The selection of the block that needs to go next in the blockchain will be determined by a consensus mechanism, where a particular node is chosen to find the next block in the chain. The hash value of each block is calculated and passed on to the next block. Any manipulations of data in the previous blocks will change the hash value of the block, which will propagate to all the other blocks and finally invalidates the blockchain. Glaser defines that blockchain has two layers of code namely the fabric layer and application layer. Fabric layer consists of the public-key infrastructure, communication layer, databases, and the execution environment for smart contracts. People who develop and maintain the fabric layer of the blockchain control the whole system. The application layer, on the other hand, comprises application logic services that are used to implement smart contracts (Glaser et al., 2014).

There are three different types of blockchains: Public blockchains, Private blockchains, and Hybrid blockchains. In Public block-chains, all the data present in the blockchain will be available to everyone in the world and anyone can join a public blockchain. Bitcoin is the largest public blockchain that is live today. The openness of public blockchains does not support any privacy for transactions. Hence, companies opt for private blockchains where the access privileges are restricted to very few individuals in the company. Participants on the blockchain need to obtain an invitation to join the blockchain and these invitations are sent by a regulatory authority within the company. Each participant in the network has a role to play in maintaining the blockchain. Hyperledger Fabric is an example of a permissioned blockchain network designed by Linux Foundation, whose purpose is to build blockchains that would cater to the needs of private companies (Jayachandra, 2017). Hybrid Blockchain or Consortium Blockchain is a blockchain where access to data is not just restricted to a single company. It is shared with some permissioned entities among a group of companies. The consensus mechanism is controlled by a pre-selected set of nodes from all the companies associated with the blockchain. An example of a Hybrid blockchain is the R3 consortium. It is a distributed database that is shared among 70 large financial institutions in the research and development of blockchain usage. Regardless of the type of blockchain, the basic functionality of blockchain is to provide validation and immutability of the transactions (Narayanan et al., 2016).

The immutability of the data in the blockchain is the key reason why we would like to use blockchain as a solution to the problem of fake information on the CVs. Once, the academic details, work experience, and other documents of a job applicant are verified and entered to the blockchain, they cannot be manipulated or erased. Hence, the employer can trust the information on the blockchain. Blockchain technology is primarily designed for multiple users in a continuous, non-centrally governed interaction among a heterogeneous group of participants (Glaser, 2017). The design of blockchain allows us to scale our solution globally. In today's globalized world, the hiring process is not just confined to one country or a geographic location, it is spread all across the world. It is not just the large multi-national companies, even many Small and Medium Enterprises (SMEs) try to hire job applicants from different countries. The process of verifying the background details of a job applicant from a different country is a challenging task involving a lot of time and money. But, the design of Blockchain technology makes the process simple and easy.

A cryptographic hash function is a mathematical function that takes an input of variable length and generates an output of fixed length that is unique to the given input. It is computationally impossible to find the input of a hash function from the hash output. Hash functions are commonly used in digital signatures and public-key cryptography, for password protection and message authentication, in key derivation functions, in pseudo-random number generators, blockchains, etc. Some of the well-known hash functions are MD5, SHA-1, SHA-256 (Narayanan et al., 2016).

Research Methodology

We used the Design Science Research Methodology (DSRM) approach for our research because it allows us to design an artifact as a solution for the given problem. Design means to create a new artifact that does not exist. Design Science Research approach is to create artifacts, constructs, models, frameworks, architectures to solve the given problem. Design Science Research Methodology allows us to create an Information Systems (IS) based solution that has the quality, utility, and efficacy to solve the problem. To solve the above-stated problem, we used the DSR approach proposed by Peffers et al, which evaluates the design science process from an Information Systems (IS) perspective (Peffers et al., 2017). Peffers et al 's paper divides the DSR process into 5 steps. They are identifying a problem, defining the objectives, designing and developing a solution, demonstrating the solution, and evaluating the solution. After the evaluation of the solution, the solution will be redesigned, redeveloped, and demonstrated iterative until the solution satisfies all objectives of the given problem.

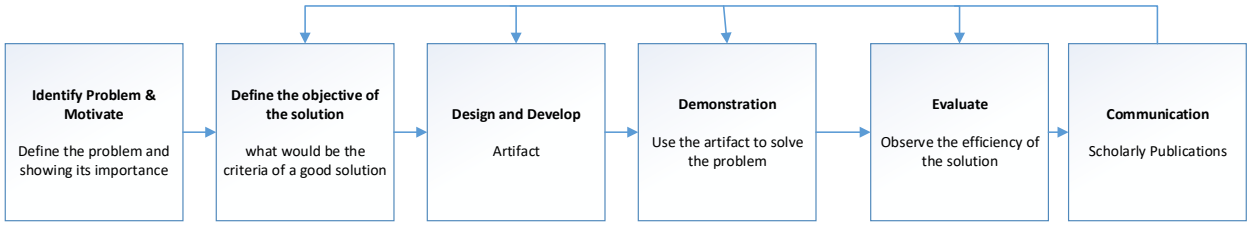

Figure. 1. Design Science Research process (Peffers et al., 2017)

For the first step, we have carefully studied the background verification process in the hiring process and define the problem as our research question. After examining the current background verification process, we identified three major objectives that our solution should satisfy in the second step. Firstly, our solution should reliably verify the background of the job applicant without any flaws. Secondly, our solution should be less time-consuming so that the companies should be able to do background verification immediately during the hiring process. Finally, our solution should be very cost-efficient so that small and medium enterprises should be able to do background verification for all their job applicants. We had several iterations in the design phase. We initially designed the solution to save the encrypted document on the blockchain using the AES algorithm (Advanced Encryption Standard) and a user interface was designed on top of the blockchain where the job applicant permits to decrypt his information for the company when applying for a job position. But, later we realized that encryption is better for the security of data during transfer over a network and hash values better for authentication (Carter & Wegman, 1981). An attacker can decrypt the content of the documents on the blockchain and compromise the security of the information of the job applicants. So, the design was modified by saving the hash values of the documents on the blockchain instead of saving the content of documents in an encrypted form on the blockchain. The modified version of the design guarantees more privacy and reliability to the solution. It is practically infeasible for the attacker to find the input of the hash value (Narayanan et al., 2016). The security of the information in the documents of the job applicants is guaranteed. Our solution would comply with the privacy laws of any country.

After designing the solution for the research problem, several latest blockchain technology platforms were evaluated to develop the solution. These platforms include Ethereum smart contracts with solidity, Corda framework, and hyperledger frameworks. After carefully analyzing the pros and cons of each of the technologies, we have decided to use hyperledger fabric for developing our solution. Hyperledger Fabric is a permissioned blockchain with a very modular structure with plug and plays components. The ledger is the sequenced record of state transactions for the blockchain where querying the data on the immutable ledger becomes easy in hyperledger fabric (Cocco & Singh, 2018).

Proposed Solution Design

A consortium blockchain is created where universities, companies, police, doctors, and certification authorities have the privilege to write the information on to the blockchain. Educational Institutions will submit the academic details such as the name of the program, list of courses taken, and grades of all their

students. All the information that you normally find on an academic transcript will be submitted to the blockchain. Companies will submit the work experience details such as years of experience, skillset, and performance ratings of all their employees on to the blockchain. Doctors can submit the results of a drug test, a psychological assessment, or other medical tests of the job applicant. Police will submit a document certifying the criminal record of the job applicant. If the job applicant does not have any criminal record, they will update his document certifying no criminal history. Certification Authority can issue a certificate of completing a training session on a skill. All these documents will be verified by an administrator node before calculating the hash values and saving them to the blockchain.

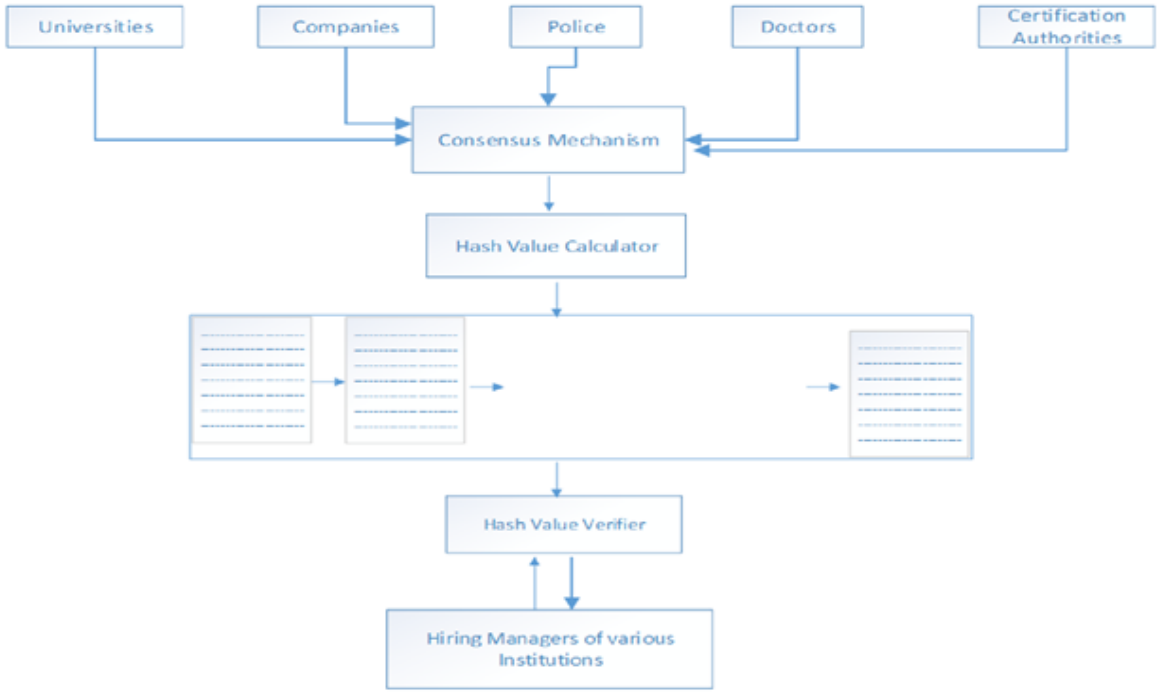

Figure. 2. Proposed Solution Design (Hash Values of the Documents from various organizations are stored in a consortium blockchain)

All the transactions (document submissions) should have a proper format and digital signature of the organizational entity. Otherwise, the transaction will be rejected. The administrator of the organization should verify and approve the transaction. Once the transaction is approved, the hash value of the document in the transaction is calculated along with the hash value of the identification (social security number plus last name) and sent to the consensus mechanism (Orderer) to update the blockchain. The hash value of the document along with the hash of the identification is stored on the blockchain. Once the hash values are stored on the blockchain, they become immutable and no one can manipulate them. When the job applicant submits his documents to the hiring manager during the hiring process, the hiring manager will upload the documents to the hash verifier web application that runs on the blockchain. The hash verifier application will compare the hash value of the uploaded document with the hash value present on the blockchain. If both of the hash values match, the application returns a value as authentic. Otherwise, it returns a value saying that the document is fake. Hence, the hiring manager can easily verify if the documents produced by the job applicant are authentic.

Prototype of the Solution

During the design process of the solution, we have decided to go with a consortium blockchain platform to facilitate various organizations to share the information. Unlike private blockchains that restrict the nodes to a single organization, a consortium blockchain consists of nodes that are distributed among a group of organizations (Shkoor, 2019). After carefully studying various blockchain technologies, we have decided

to use hyperledger fabric for our use case. Hyperledger Fabric is an open-source permissioned distributed ledger technology (DLT) platform, which offers high modularity supporting external plugin components, performance scalability, and configurable architecture compared to other blockchain technologies (Hyperledger, 2019). The front-end of the application is built using HTML and Javascript. Python code was used to calculate the hash value of the document.

Hyperledger fabric consists of several components. The organizations that take part in building hyperledger fabric network are called members. In our use case, universities, companies, doctors, police, and certification authorities are referred to as members. Each of the members in the consortium blockchain would be provided with at least three entities Peer, Administrator, and Certification Authority. Peers are referred to individual nodes that can initiate a transaction and host the ledger to query and update the application through smart contracts (Hyperledger, 2019). A peer is responsible for submitting the document to the blockchain. The administrator of the organization verifies the authenticity of the document and approves it. Then, the hash value of the document along with the hash of the identification (Social Security Number + Lastname) will be updated on the blockchain by the orderer and the transaction is updated by all the orderers in the network. We use the SHA-256 algorithm to calculate the hash of the document. The administrator is also responsible for invalidating an entry that is mistakenly updated by the peer. Certification Authority is responsible for giving certificates to the administrators and peers. Apart from peers, administrators, and certification authority, we have orderer nodes which are responsible for ordering the transactions into a well-defined order and package them into blocks. This group of orderer nodes together are called as ordering services. Once all the transactions are saved into blocks, these blocks are distributed to all the other peers in the network (Hyperledger, 2019). A recruiter of an organization will act as the "Verifier" of a job applicant's document and obtained a verifier certificate from the verifier organization.

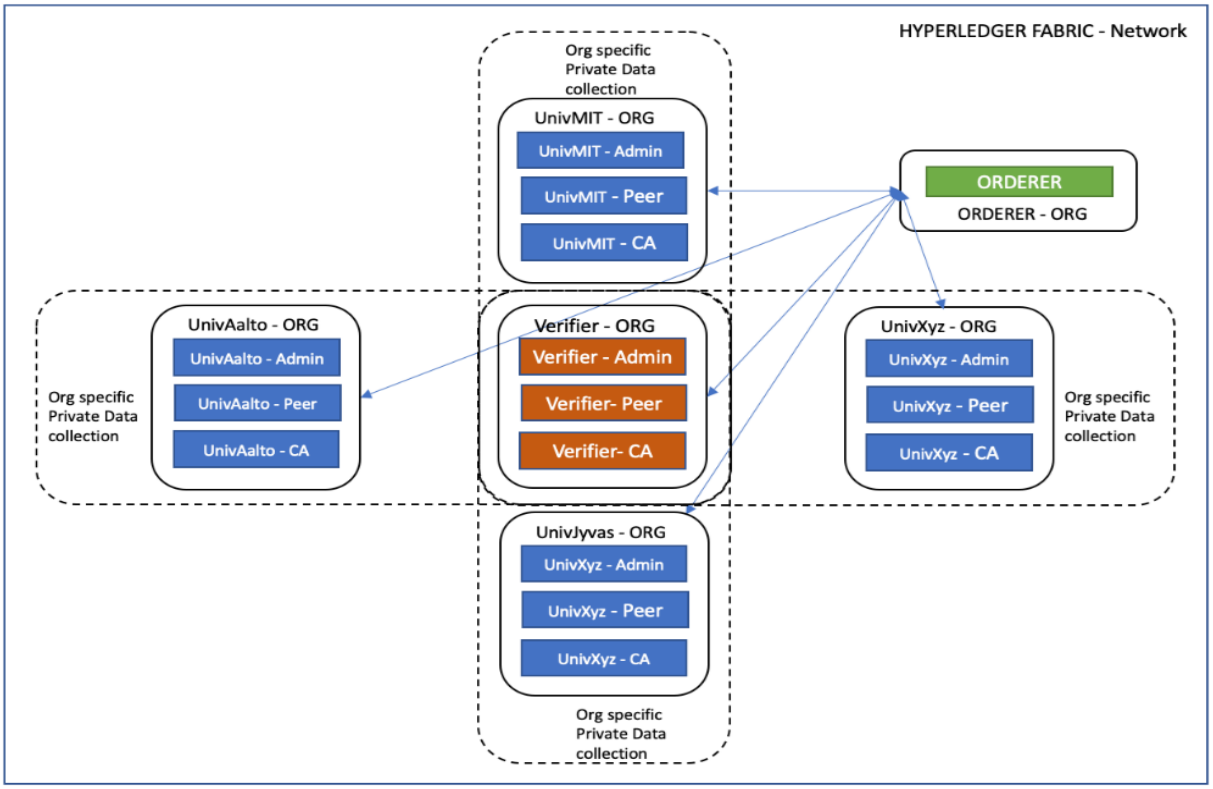

Figure. 3. Architecture of the Hyperledger Fabric Consortium Blockchain depicting the Peer, Admin, Certification Authority, and Orderer Nodes

Data entered into the blockchain consists of two fields: the hash value of the identification, and the hash value of the document. The following figure represents the data stored on each of the blocks. The last two

fields IsValid, Reason for Invalidity are used if the hash value of a wrong document is mistakenly entered in the blockchain. The value entered in the blockchain cannot be deleted and IsValid is set to TRUE by default. However, an administrator peer of the organization will have the privilege to invalidate an entry in the blockchain and provide an explanation for the inaccuracy.

Hash Value of the Identification	*Hash Value of the Document*	*IsValid*	*Reason for Invalidity*
3639efcd08abb273b1619e82e78c29a7df02c1051b1820e99fc395dcaa3326b8	99d7311e4bb67c98c3f5da9e14cab4e1a1f59830c7578876d2d4fce87461ec2d	TRUE	
d1b65e1db356712f07bcfe3678d2bc373926f6e3c18d517588cb641dde6059a0	65794574b4e3838ebe0914a6fa6c4eea48bc817af6c883b43208d6c60c61ce31	TRUE	
1f1fb0690376941ea663b89fcc2a2c42d13aa6ce27d59e94fe4669c900b7a2e6	3e7ea869af789180199057d601e94a16a921ae3a621ab27b8091fce387d1d320	FALSE	Mistakenly submitted a wrong document by Mr X and mistakenly validited by Mr Y

Figure. 4. Data on the Blockchain

The solution for the problem can be found in the Github page mentioned in the footnote[1]. The implementation details on how to install the solution are clearly stated on the Github page.

Workflow of the Solution

The workflow of the proposed solution starts with the peer of an organization submitting a document to the administrator. The administrator of that organization verifies the document and either approves it or rejects it. If the document is approved, the hash values of the identification and the document are sent to the orderer with the approval of the administrator. Orderer verifies the administrator's approval and updates the entry in the blockchain. Once the entry is entered into the blockchain, other orderers in the consortium blockchain will update the hash values of the document. When a job applicant approaches an organization for a position, his documents are submitted to the recruiter. The recruiter (Verifier) will verify the authenticity of the document provided by the job applicant using the web application. The recruiter (Verifier) does not have direct access to all the hash values in the blockchain. He/She can only query the data on the blockchain. The recruiter shall only submit the Identification (Social Security Number and Lastname) and the document (Eg: Transcript) on the web interface and shall receive a message if the document is authentic.

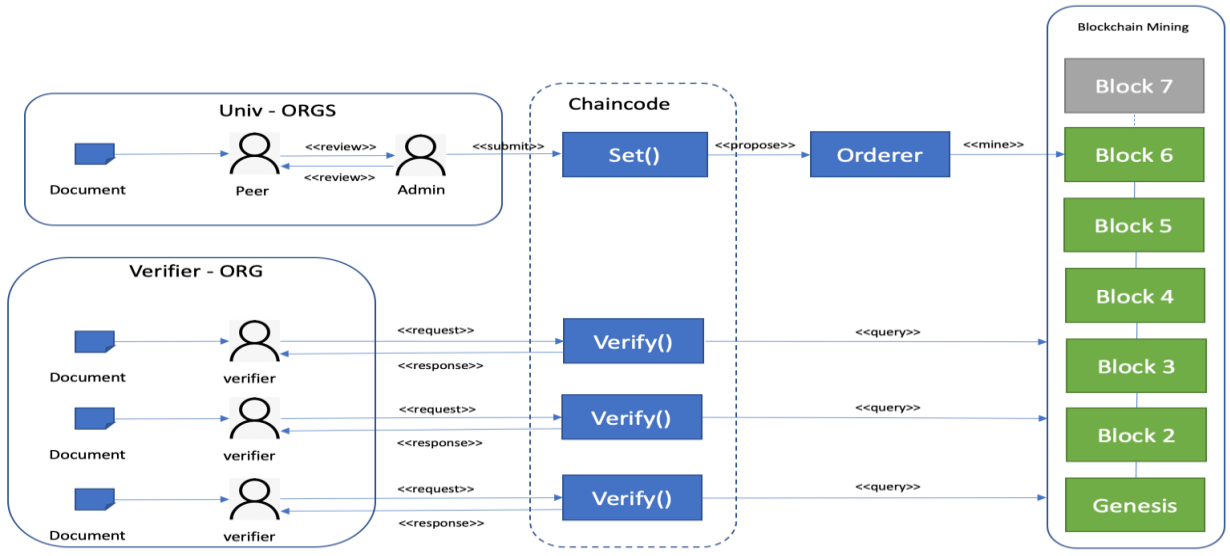

Figure. 5. Workflow of the Solution

[1] Link to Github: https://github.com/maniankara/desrist2020-demo

Novelty of the Solution

A similar solution can be designed using a central database application instead of a blockchain. But, such a system does not guarantee that data is not manipulated by someone who has access to the system (Internal hacking). Despite having several layers of security, it is still possible for an outside attacker to manipulate the data (External hacking). The immutability of the data and the distributed nature of the blockchain serves as a better option compared to a centralized database system (Tabora, 2018). The immutability property of the blockchain provides data integrity. Data is distributed across several nodes in the blockchain, which makes it easier and faster for hiring managers to access it and improves the availability of data. By using the hash values of the documents, we can authenticate the documents, while making them confidential. Thus, our solution satisfies the CIA (Confidentiality, Integrity, and Availability) properties, which are fundamental elements of security controls in information systems (Coss & Samonas, 2014).

With the help of blockchain technology, our solution is globally scalable and can act as a single global platform for hiring managers to verify the background details of the job applicants from various geographic locations. When hiring a job applicant from a different country, it is extremely difficult to verify the documents provided by him. When the job applicant finishes his degree in his home country, his university will submit the transcript document to the blockchain and the hash value of the document is stored on the blockchain. Once the hash value of the transcript document is stored on the blockchain, it can be verified by any company in any geographic location.

Advantages of the Proposed Solution

The proposed solution has several advantages compared with the existing hiring process. As mentioned in the previous sections, the current process is very costly, time-consuming, and inefficient. In this section, we will discuss in detail how our proposed system solves those issues.

Cost Reduction In the proposed solution, the hiring manager needs to pay a significantly low amount of money for the verification of each document using the hash verifier application. This money will be rewarded to the organization entities that verified the transaction and saved the hash value of the document on to the blockchain. This low-cost background verification process will help the small and medium scale enterprises to verify the background details of the job applicants during the hiring process. Hence, it will help the companies to select the truly skilled employees during the hiring process.

Time-Saving The proposed solution is far less time-consuming than any other background verification systems that exist today. Hiring managers can immediately verify the authenticity of the documents submitted by the job applicant during the hiring process itself. Most of the current background verification processes will take a lot of time, which can delay the hiring process. In some cases, the organization starts the verification process after hiring the employee. Then, the companies might lose a lot of money, time, and resources by hiring the wrong candidate for the job position.

Efficient Process The proposed solution is very efficient in verifying the documents provided by the job applicant. It is practically infeasible to manipulate a document without changing the hash value of it (Narayanan et al., 2016). The hash values entered in the blockchain cannot be tampered. Most of the current background verification systems are done manually, which is prone to errors or manipulations. But, our proposed solution will work efficiently by overcoming all the problems of the manual process.

Privacy We are saving the hash value of the documents of the job applicants on the blockchain instead of the actual documents in the encrypted form. Hence, all the information about job applicants is completely secure. Secondly, we are using a permissioned blockchain where known organizations are allowed to access the hash values from secured nodes. Hence, our solution will provide high privacy for the information. Though the GDPR considers that hash values only accomplish pseudonymisation, the use of permissioned blockchain would provide the required privacy for the data (Consortium, 2018).

Global Scalability Our solution can include organizations from any country in the world. Once the framework is set up, the scalability is very easy on hyperledger fabric (Hyperledger, 2019). Hence, the

given solution is not just restricted to any one geographic location and the hiring process of job applicants becomes an easy task. Once a proper organizational ecosystem is built around our solution, it can be used globally as a single system for the verification of information provided by the job applicants.

Conclusion

This paper aims to develop a solution for the background verification process of job applicants during the hiring process using blockchain technology. The current verification system used by many multinational companies is inefficient, time-consuming, and costly. So, many small and medium-size companies do not go for background verification during the hiring process. The paper proposes the use of Information Systems (IS) to resolve the problems with the background verification process using the design science research methodology. We have to build a blockchain ecosystem where only the hash values of the documents are saved on the blockchain without saving the original document. This will protect the privacy of the information of the job applicant as it is impossible to guess the input of the hash function by looking at the hash output (Bellare et al., 1996). Our solution is easily scalable to any geographic location. Our solution will be an efficient tool for hiring managers in selecting the right job applicant. Our solution not only reduces the cost of doing the background verification but also eliminates the wastage of time and the other resources involved in hiring a job applicant with false qualifications. Our solution is not just restricted for the document verification of the information on the CV, it can be easily extended to the applications in other domains. For instance, with some changes to our solution, we can use the same solution for the verification of the land record documents. Hence, our solution is very generic, that can be implemented in various other domains.

References

Bangerter, A., Roulin, N., & König, C. J. 2012. "Personnel Selection as a Signaling Game." *Journal of Applied Psychology*, *97*(4), 719–738. https://doi.org/10.1037/a0026078

Bellare, M., Canetti, R., & Krawczyk, H. 1996. "Keying hash functions for message authentication" *in Proccedings of 16th Annual International Cryptology Conference Adv.*, 1–15.

Bonanni, C., Drysdale, D., Hughes, A., & Doyle, P. 2011. "Employee Background Verification: The Cross-Referencing Effect". *International Business & Economics Research Journal (IBER)*, *5*(11), 1–8. https://doi.org/10.19030/iber.v5i11.3519

Bourne, M. 2015. "Who Are You Hiring? The Shocking Cost of Résumé Fraud." Retrieved from https://www.business.com/articles/the-shocking-cost-of-resume-fraud/

Brown, M. 2017. "The Drawbacks and Deceptions of LinkedIn." Retrieved from https://lendedu.com/blog/drawbacks-deceptions-linkedin/

Buckhoff, T. 2003. "Preventing fraud by conducting background checks." *The CPA Journal*, *73*(11), 52.

Campbell, R. 2015. "Lying on Your CV: The Facts." Retrieved from https://www.topuniversities.com/blog/lying-your-cv-facts

Carter, L. L., & Wegman, M. N. 1981. "New hash functions and their use in authentication and set equality." *Journal of Computer and System Sciences*, *22*, 265–279.

Cocco, S., & Singh, G. 2018. "Top 6 technical advantages of Hyperledger Fabric for blockchain networks." Retrieved from https://developer.ibm.com/technologies/blockchain/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/

Consortium, L. 2018. "How does the EU's GDPR apply to hashed data on the blockchain?" Retrieved from https://legalconsortium.org/uncategorized/how-does-the-eus-gdpr-view-hashed-data-on-the-blockchain/

Coss, D. Samonas, S. 2014. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security*, *10*(3), 21–45.

Glaser, F. 2017. "Pervasive Decentralisation of Digital Infrastructures : A Framework for Blockchain

enabled System and Use Case Analysis", *in Proceedings of 50th Hawaii International Conference on System Sciences* 1543–1552.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. 2014. "Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions." *in Proceedings of Twenty Second European Conference on Information Systems*, 1–14.

Hyperledger. 2019. "Hyperledger Fabric Documentation. *PDF Download Release 1.4*. hyperledger-fabric." Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-1.4/

Ina van der Merwe. 2015. "Why you should never lie on your CV." Retrieved from https://city-press.news24.com/Personal-Finance/why-you-should-never-lie-on-your-cv-20151115

Jayachandra, P. 2017. "The difference between public and private blockchain." Retrieved from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Jund- Ming, W. 2000. "Effective employment screening practices." *Management Research News*, *23*(5/6), 73–81. https://doi.org/10.1108/01409170010782055

Keller, S. 2006. "Employee screening: A real-world cost/benefit analysis." *Risk Management*, *51*(11), 28–32.

Kraps, L. 2015. "The Legal Risks of Lying on Your Resume." Retrieved from https://www.addrc.org/the-legal-risks-of-lying-on-your-resume/

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* Princeton, NJ, Princeton University Press.

O'Donnell, J. 2017. "Resumes. Here's How to Spot a Dishonest Candidate." Retrieved from https://www.inc.com/jt-odonnell/staggering-85-of-job-applicants-lying-on-resumes-.html

Office, E. 2013. "Lie On Your Resume And You Could Be Slapped With A $5,000 Fine." Retrieved from https://employmentoffice.com.au/lie-on-your-resume-and-you-could-be-slapped-with-a-5000-fine/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. 2017. "A Design Science Research Methodology for Information Systems Research", *Journal of Management Information Systems,* 24(3), 45-78. https://doi.org/10.2753/MIS0742-1222240302

Shkoor, M. A. 2019. "Everything You Need to Know About Public, Private, and Consortium Blockchain." Retrieved from https://medium.com/swlh/everything-you-need-to-know-about-public-private-and-consortium-blockchain-54821c159c7a

Shukla, A. 2014. "Watch out for fake degrees." Retrieved from http://www.thehindu.com/features/education/watch-out-for-fake-degrees/article5743087.ece

Tabora, V. 2018. "Databases and Blockchains, The Difference Is In Their Purpose And Design." Retrieved from https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b

White, M. 2015. "You Won't Believe How Many People Lie on Their Resumes." Retrieved from https://money.com/how-many-people-lie-resumes/