International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Alumnichain: Blockchain Based Records Verification Service

Siddharth Badyal, Akash Chowdhary

Abstract*:The proposed system is a ledger of student qualifications that aims at making recruitment processes simpler for the universities, recruiters as well as the students. Instead of continuing with the traditional way, of background checks that take even days worth of time and cost a lot of money, we have proposed an instant student background verification service that allows verification of data by recruiters, that has been signed by the university and uploaded to an immutable, secure ledger called the blockchain or as we call it, the Alumnichain. The students simply have to include a code provided to them, to their CVs which can be scanned by the recruiters, to have all student data instantly verified. The data stored on the network is not in plaintext and is encrypted to ensure security against potential data thefts. All this is achieved through a blockchain implementation of the above described use case, which has proved to be a solution to so many problems since its inception, starting with Bitcoin in 2008.

***Keywords* :blockchain, decentralized, ledger, peer-to-peer .**

I. INTRODUCTION

A. *Background*

Recruitment processes is one area, where despite of all the technical advancements we have seen over the last decade, very little has changed and things are done the same way they once were, through manual background checks by recruiters that takes a long time. According to statistics, resume fraud has weighed in on the IT industry and one in five CVs contain fake information.[1] Often small recruiters and even the big recruiters, when under pressure from management do not conduct a proper background check due to the time and expenses involved, which results in people with fake CVs getting hired, while genuine candidates miss out on the opportunities. Since, it is getting tougher to get jobs these days as most recruiters demand freshers with higher skill [2], lying on CVs appears tempting to a lot of freshers. It is popular knowledge that Scott Thompson, former CEO of Yahoo! lied on his CV about holding a Computer Science degree and had to leave the company when the news got out.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Siddharth Badyal*, B.Tech. CSE, SRM Institute of Science and Technology, Kattankulathur campus, Chennai, Tamil nadu, 603210. Email: siddharthforwork@gmail.com
Akash Chowdhary, B.Tech. CSE, SRM Institute of Science and Technology, Kattankulathur campus, Chennai, Tamil nadu, 603210. Email: chowdharyakash97@gmail.com

Lying on the resume can mean severe consequences to the candidate, if found out and is otherwise harmful to the hiring firm and the genuine candidates that get left out.

B. Motivation

Academic fraud still continues to be a problem simply because it's not highly prioritised by most of the companies due to various reasons. The processes involved are long, complicated and really tedious which simply does not seem worth the effort and time when compared to thebenefits it provides for smaller companies. The lack of competition in this domain is also a cause for the high costs for verification requests, and from our point of view, everyone stands to benefit from a cheaper service that can simplify these verification processes. There is the National Skills registry(NSR), that holds candidate qualification data, but it has a long way to go. Not a lot of companies use their services, except for some of the mass recruiters.[3] Most companies still rely on their own background processes. Moreover, the data on the NSR is held centrally, which is less secure than the way a blockchain stores data.

C. Present System (Limitations)

Currently the recruitment space does not have a single service to depend on and companies usually conduct their own background checks which has resulted into a complex system that poses several limitations as:

- Recruiters conduct manual checks that are tedious and not so cost effective.
- Small firms and when under time constraints even the big firms often skip out on these background checks or are less than thorough which, results in the wrong candidates being hired while the genuine ones miss out.
- The universities also have to go through a great deal of administrative work to maintain these records and manually query them for every verification request.
- Even if a more convenient service exists, like the NSR [3] it has not seen widespread adoption and is not mandatory to register for the students/freshers.
- Furthermore, the data stored by such central services is far less secure, than what is being proposed.

D. Proposed System

AlumniChain is a blockChain based service that we have proposed as an improvement over the existing systems, that shall work to benefit all involved parties; the recruiters, the university and the graduates.

Taking inspiration from Gradbase [10], the project aims to deploy a permissioned blockchain, to securely hold academic records on university peer nodes, for instant and possibly fee-free verification of records by recruiters.

1) For Universities:

- There is no need for all the time spent manually verifying each request, by looking through the registry since, each request will be automatically verified.
- The service delivers a very convenient and intuitive UX for managing the qualifications data through an online form interface for the university, that allows managing individual records as well as bulk upload of records to sign and upload multiple records to the network at once.
- The service shall offer all required operations on the qualifications data from signing to updation and revocation of records.
- The data collected is well protected by not being stored as plaintext but in encrypted format and on a decentralized network called a blockchain, that has no central point of failure.

2) For Recruiters:

- Offer an easy one-click way for verification of records, which for the worst case may require recruiter to fill a form as opposed to the current tedious process that can take upto days.
- Instantly verify records by querying the blockchain with the fetched block code, and subsequently comparing data.

3) For Graduates:

- A great way to add credibility to their qualifications, by simply adding the unique code to their profile.
- Relieve them of the hassle of obtaining attestations from the university for their qualifications, which can be a lot of effort.

II. METHODOLOGY

A. Architectural Implementation

The proposed system is implemented using blockchain technology which is pretty complex in itself. So, to decide on an implementation architecture, some of the most common and one of the first blockchain applications were studied, such as the bitcoin and the ethereum blockchain. The ethereum blockchain implements a more simpler and relevant system for user accounts with regards to our application. It's because of this implementation that the ethereum blockchain also allows smart contracts on the network that allow for developers to de-ploy their own individual applications on the same blockchain. the same has also been considered for implementation of our proposed system.[6]. The bitcoin blockchain on the other hand, although builds on some of the key concepts being the first blockchain application ever, implements a more complex system for user accounts with UTXOs being the most basic unit that defines the state of the blockchain. Several UTXOs makeup a transaction and each account basically just keeps track of the incoming and outgoing UTXOs to determine each accounts balance. This is depicted well in Fig (2). Since, our system does not involve transactions as in case of bitcoin, implementing such a system has no use in our applications, whatsover. So the key takeaways were the concepts of a

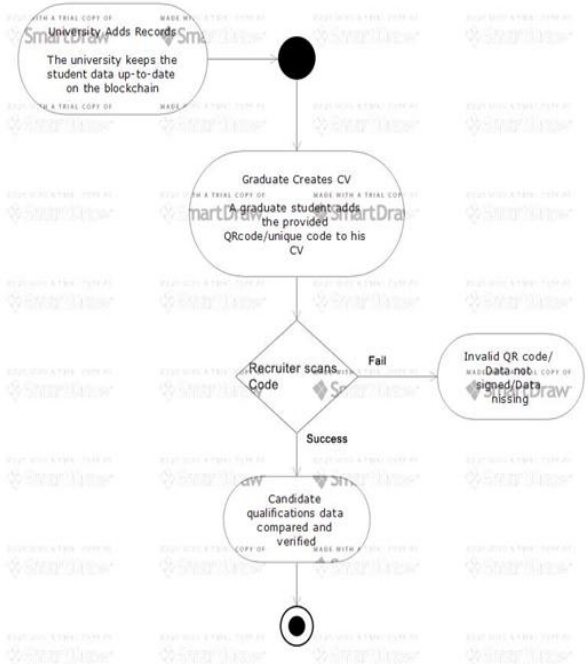

Fig. 1) Activity flow diagram for the process.

consensus protocol and a basic understanding of just how distributed networks work.[4]. The system is proposed to be coded in Go language because of its javascript like syntax, for ease. It's also very light weight and efficient which was also a deciding factor.[8]

B. Proof-of-Concept Implementation

The proof of concept will be deployed using the open source version of the Hyperledger fabric which is one the products of the Linux Hyperledger Consortium, meant specifically for building blockchain applications with ease and efficiency.[7]. The platform neatly packages modules that are necessary for blockchain deployment which can be configured and setup easily using the command line interface that comes with the hyperledger composer, which we have employed.

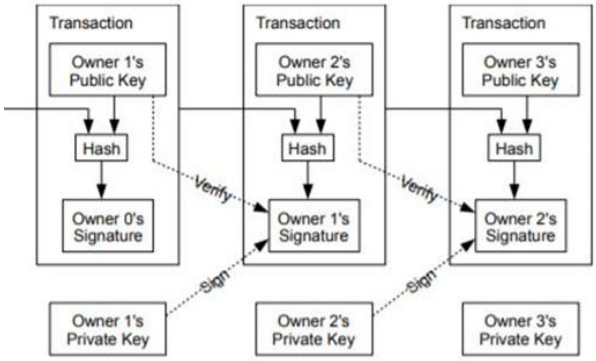

Fig. 2) Bitcoin's implementation pf transaction signing and chain creation.

Hyper-ledger internalizes the transaction signing, validation and the consesus protocol while allowing for full customizability in case a custom consensus algorithm maybe desired. This is achieved through the Fabric CA, peers, and the ordererwhich collectively take

Table I: Literature Survey Table

Sl. No.	PaperTitle	Takeaway
1)	Bitcoin: A Peer-to-Peer Electronic Cash System	The author has built a peer-to-peer electronic cash system that laid basis for the decentralised p2p network we now know as the blockchain. He goes on to elaborate on the technicalities of what he did for the consensus protocol, validation and various other mechanisms.
2)	SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies	The authors have written on various challenges that are faced by cryptocurrencies such as bitcoin by drawing out the various properties of the system, discovered attacks and the future challenges pertaining to scalability, privacy and general upkeep. Several alternate mechanisms for the consensus protocol, key management and disintermediation strategies with a detailed comparison are given.
3)	Ethereum White Paper: A next generation Smart Contract and Decentralised Application Platform	The author has built the revolutionary blockchain technology known as the Ethereum blockchain. He believes that theres a major shift in the applications of the blockchain technology, which is why the Ethereum network introduced the smart contracts feature that enables a person to run any business logic on top of the Ethereum blockchain itself, thus, providing an easier way of creating Decentralized applications. A lot of these applications are what we today call as tokens or altcoins.
4)	Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains	The authors have wrote on the open source extensible blockchain framework known as the Hyperledger fabric, that was developed by IBM and hosted by the linux foundation. The framework offers, by far, the most hassle-free solution for enterprises creating blockchain applications, that doesnt depend on any underlying currency, or some domain specific language.
5)	Why build a blockchain in Go	The author from his experience in building the karachain highlights the key features of the Go language by google, because of which Go has become the new go to language for blockchain development.
6)	IPFS - Content Addressed, Versioned, P2P File System	The author has highlighted the various key features of the interplanetary file system, which is a P2P distributed file system, that has seen an important application in many of the blockchain projects.

care of generating key pairs for network participants, generating transaction proposals, signing and verifying them, and reflecting the endorsed transactions on the ledger respectively.[7] The essence of the network lies in the Business network archive, required for providing the network definition. It consists of a model file, that models all the assets, participants and transaction types the network can have, and optionally events. A logic.js file describes the logic for processing of transactions defined in the model file and lastly an .acl file, describes the permission rules as per the roles of participants interacting with the network. As such a typical BNA structure maybe depicted as in diagram Fig. (3).

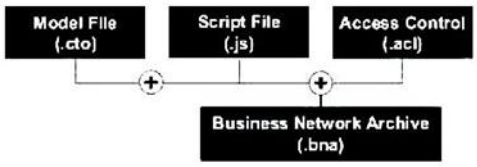

Fig. 3) Business network archive (Block Diagram)

Based on the network definiton, a blockchain is deployed and APIs are generated for interaction with the network, to retrieve data, upload or remove assets, perform trasactions and do possibly more. As a proof of concept the network only exists on one peer but can be easily scaled to incorporate more peers if required.

The business network archive only defines the business application structure and code, and interacts with the underlying pre-defined chaincode of the hyperledger. However, configuring the network down to every aspect is doable through various tools made available by the hyperledger itself. The certificate generation process for every network participant can be performed manually through the configtxgen and crytpogen commands through the composer command line. The chaincode language that is to be followed can also be configured at the time of network initiation, through simple commands all of which is discussed in depth in the hyperledgerdocumentation[7].

The hardware aspects of the network can also be configured quite easily. While, the orderer has to be configured before the network setup for the number of peers it must have, and with what organisation, the submitting peers can join the network relatively easily, by just joining an existing channel. Each organisation is provided with a root certificate authority, ca-cert that generates keys for that organisation's peers. And, once the network is instantiated the public keys from each peers are stored in the genesis block for easy verification in future. The in-depth knowledge of this can also be gained from the hyperledgerdocumentation[7].

As such the working of the underlying Hyperledger suite and consequently our blockchain system is as depicted in fig.(4).

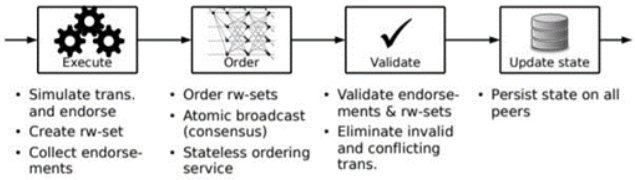

Fig. 4) Execute-order-validate architecture of fabric.

III. RESULT ANALYSIS

An implementation of the blockchain technology that comes closest to our implementation, which is also the root of our inspiration is the GradBaseSystem.

The Grad base system works on top of the bitcoin blockchain, working to encapsulate student record data within bitcoin transaction blocks. When evaluated against the GradBase system our system appears to outperform them on several metrics:

- Security aspect: Unlike GradBase which employs a Bitcoin blockchain which is public , our system uses a permissioned blockchain with access control rules.
- Time taken for transaction processing: Since our system uses a dedicated blockchain blocks don't need to be mined and records are updated instantly.
- Bitcoin blockchain network would involve transaction costs.Only costs incurred in our system would be in setting up the network and maintaining it.
- The computational overhead is also way lesser for operation of a permissioned blockchain network, which is proposed.

From evaluation against existing systems it can be inferred that the existing security issues as well as core issues about academic fraud can be successfully solved with our proposed system.

IV. CONCLUSION

On studying the blockchain workings of one of the first blockchains ever implemented a basic idea is drawn out regarding the technological requirements for implementation of the proposed system. The understanding of how blockchain works, and use smart contracts was important to come up with a development path for proposed system.

Open source version of the Linux hyperledger is used to build and deploy our proof of concept, blockchain network and this was a clear choice because of the vast set of tools that it offers that really simplifies the development process and is easily scalable.

ACKNOWLEDGMENT

We express our profound feeling of appreciation to our regarded and learned guide, Asst. Prof. Ms. M Hema for their profitable help and direction, we are appreciative to them for the support they have given us in finishing the venture. We are likewise appreciative to regarded Prof. Dr. B. Amutha, HOD (CSE) and to our regarded Director (E and T) Dr. C. Muthamizhchelvan for allowing us to use all the vital offices of the foundation. We are additionally appreciative to the various faculty and staff individuals from our college for their caring co-activity and help. Finally, we might want to express our profound gratefulness towards our schoolmates and our indebtness to our folks for giving us the ethical help and consolation.

REFERENCES

1. AUTHBRIDGE, HTTPS://WWW.AUTHBRIDGE.COM/NEWS/RESUME-FRAUD-WEIGHS-ON-INDIAN-IT-INDUSTRY-ONE-IN-FIVE-CVS-CONTAIN-FAKE-INFORMATION/ HTTPS://WWW.AUTHBRIDGE.COM/NEWS/RESUME-FRAUD-WEIGHS-ON-INDIAN-IT-INDUSTRY-ONE-IN-FIVE-CVS-CONTAIN-FAKE-INFORMATION/
2. The Wire, https://thewire.in/economy/jobs-private-engineering-colleges-tough
3. National Skills Registry, https://nationalskillsregistry.com/
4. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, satoshin@gmx.com www.bitcoin.org
5. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten, SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2015, pp. 104-121. doi:10.1109/SP.2015.14
6. VitalikButerin, Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform, http://blog.lavoiedubitcoin.info/public/Bibliotheque/Ethereum White-Paper.pdf
7. Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Kon-stantinosChristidis, Angelo De Caro, David Enyeart, Christopher Fer-ris, Gennady Laventman, YacovManevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith,Alessandro Sorniotti, ChrysoulaStathakopoulou, Marko Vukoli, Sharon Weed, Jason Yellick, Hyperledger Fabric: A Distributed Operating Sys-tem for Permissioned Blockchains, EuroSys '18 Proceedings of the Thirteenth EuroSys Conference Article No. 30 Porto, Portugal April 23-26, 2018 ACM New York, NY, USA 2018 ISBN: 978-1-4503-5584-1 doi¿10.1145/3190508.3190538
8. Syed Jafar Naqvi, Why build a blockchain in Go, https://medium.com/karachain/why-i-am-building-a-blockchain-in-go-6395a60b24dd
9. Benet, Juan IPFS - Content Addressed, Versioned, P2P File System, 2014/07/14 arXiv:1407.3561 [cs.NI]
10. Cedric Colle, Alberto De Capitani, Kenneth Lindroos, Andrej Maris, Tomas Virgl, KacperZylkaGradbase: Decentralised academic record verification using the Bitcoin blockchain,2015/01/12https://www.doc.ic.ac.uk/teaching/distinguished-projects/2015/l.colle.pdf
11. KENTAROHTOYODA1,(Member,IEEE), P.TAKISMATHIOPOULOS, (Senior Member,IEEE), IWAO SASASE, (Senior Member, IEEE), AND TOMOAKI OHTSUKI, (Senior Member, IEEE), Keio University, Kanagawa 223-8522, Japan. Nationaland Kapodestrian University of Athens, 15784 Athens, Greece Corresponding author: Kentaroh Toyoda (toyoda@ohtsuki.ics.keio.ac.jp) A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain,https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7961146

AUTHORS PROFILE

Siddharth Badyal, received his B.Tech. degree in computer science and engineering from SRM Institute Of Science and Technology, Kattankulathur, India, in May 2019. He is an IBM certified blockchain developer and is certified to hold in-depth knowledge of blockchain concepts and existing blockchain systems. He is deeply interestedin exploring blockchain technology further, and to reform various industries that can be made more secure and peer-controlled, provide more functionality and efficiency with a decentralized architecture as opposed to conventional centralized systems. Having studied and worked with cryptocurrenies, he also vests great interests in the fintech domain and the possible applications of blockchain, therein.

Akash Chowdhary, received his B.Tech. degree in computer science and engineering from SRM Institute Of Science and Technology, Kattankulathur, India, in May 2019. Since then, he has been with Cerner Healthcare Solutions India Pvt Ltd employed as a Software Engineer. His current research interests include blockchain, blockchain in fintech and its applications in a decentralized universe. He believes in the idea of a decentralized universe giving back the control to the people. He has attended several workshops on blockchain. He aims to keep exploring pioneering technologies in the field of computer science to introduce solutions to tackle real life problems.