Blockchain technology: A solution to plight of Nepalese migrant workers in foreign employment

SIJAN PANDEY1* and SIRISH PACHHAI1

1Department of Computer Science, St. Xavier’s College, Maitighar, Kathmandu, Nepal
*Corresponding Author Email: pandeysijan10@gmail.com
http://dx.doi.org/10.22147/jusps-B/301101

Acceptance Date 9th October, 2018, Online Publication Date 2nd November, 2018

Abstract

Interest in blockchain technology, the technology behind Bitcoin, has increased recently. Blockchain enables non trusting users in a distributed peer to peer network to agree to a single set of record without the need of a trusted middleman. Data stored in a blockchain is an immutable history of authentic records and is easily verifiable. This paper reviews the fundamentals of blockchain technology.

Foreign employment remains highly sought after option for Nepalese workers. However, they have been facing frauds related to contract substitution, misrepresentation of terms and conditions and overcharging of fees leaving them vulnerable to exploitation. This paper reviews foreign employment procedure in Nepal and problems faced by Nepalese migrant workers. This paper also proposes and analyses a solution based on blockchain technology to form an authentic, tamper proof, verifiable record of contracts for enabling a robust, accessible, transparent, organized and safe foreign employment procedure in Nepal.

Key words: Blockchain; Nepalese migrant workers; immutable contract; verifiability

Introduction

Blockchain is a distributed database structure where all the data is maintained in a public ledger and the ledger is shared among all the nodes participating in the network. Every node in the network keeps a copy of the entire ledger and confirms it. Blockchain technology was developed with the aim of keeping the transaction system decentralized with no involvement of middleman, which controls and manages all the data and transactions in the system, between transacting entities. Because of achieving same functionality as of centralized systems even in decentralized network systems, blockchain have been applied in fields - like finance, health care, utilities, real estate and government sector - beyond crypto currency.
Labor migration for foreign employment from Nepal till 20th century was confined to India, which shares an open border with Nepal. 3,605 labor permits were issued in 1993/94 to countries other than India. However, since 2001, more than 100,000 permits have been issued annually. 3,509,633 labor permits were issued by Department of Foreign Employment from fiscal years 2008/09 to 2016/17. This data excludes number of workers migrating to Republic of Korea through government-to-government Employment Permit System. Not only the number of workers acquiring new permits but also the number of workers renewing their permits has remained high. 1,196,687 labor permits were renewed in six fiscal years since 2011/12. Number of workers in Nepal seeking foreign employment has significantly increased in recent years as adequate economic growth has not been achieved in Nepal to provide jobs to the growing population.

Procedure of migration for foreign employment:

Labor migration process for foreign employment in Nepal is carried out according to procedures outlined by the Foreign Employment Act of Nepal 2007.

![Fig.1 Labor migration procedure via recruitment agencies in Nepal](image-url)

FEA also permits migrant worker to undertake foreign employment process individually by finding job on their own instead of proceeding through recruitment agencies. However, use of a recruitment agency has been preferred by the migrants. 82.52% of all labor permits over the fiscal years 2008/09 to 2016/17 were issued to migrants that used this mode of migration. Most of the prospective workers get contacted to the recruitment agencies via individual local agents. According to ILO’s study, 36 percent of migrants were first contacted through local agents. In case of Dhanusa district, this number rose to 96 percent. Generally, prospective migrants in Kathmandu valley directly contact recruitment agencies whereas those in other parts of the country get contacted through local agents.
Problems faced by laborers:

Most of the problems experienced by the workers are due to recruitment agencies, individual agents, manpower agencies in destination countries and employers. Charging of excessive fees, misrepresenting terms and conditions of employment and fraud by not providing correct pre-departure documents are common problems that migrants have faced. About 70% of workers responded that terms and conditions were different than agreed before departure. Individual agents that play huge role in initiating prospective migrants’ recruitment process by contacting them with recruitment agencies have often been linked to fraud, misrepresentation and overcharging of fees. Most of the distress reports filed by laborers have been against recruitment agencies and individual agents who deceived the migrants during employment process. The workers have faced “high level of exploitation due to contract substitution and deception of working and living conditions, overcharging for services provided and fraud by non-compliance with the employment agreement”. Many end up in jobs different from what they signed up for, are paid salaries lower than what they were assured and do not get the benefits they were promised. According to a study, workers weren’t provided contract signed between them and the recruitment agency at all. They mentioned that recruitment agency said them that there was no such requirement. Although contract signed between worker and employer were provided, only 5 out of 54 workers received it several days before their departure so that they had enough time to go through the terms and conditions mentioned. In addition, those contracts were in the language which the migrants weren’t comfortable with (English and Arabic) and were incomplete in terms of the description of terms and conditions and other information about the job. Recruiters can substitute the contract; misrepresent terms and conditions as contracts aren’t in the language which migrants understand. The major issue with having false contracts or no contracts at all is that the migrant workers are not in the position to produce those documents for supporting their claim and seeking redress if wages or working conditions are different from that is mutually agreed. Contracts act as an evidence of mutual agreement. Another common harm that migrants face is confiscation of documents by employers. About 63% of workers mentioned that their documents were confiscated. This keeps migrants even more vulnerable to exploitation and seeking redress can be difficult without supporting documents.

Fundamentals of blockchain technology:

Blockchain comprises sequence of blocks linked to each other in linear and chronological order. Blocks hold data in the blockchain. A new block is generated when data stored in the block reaches its size limit. The newly generated block is linked to previous block (parent block) using hash value of the previous block which is produced using cryptographic hash function.

Cryptographic hash function is an algorithm which is used to verify the authenticity of a data. The piece of data is passed through the function and an alphanumeric hash value of fixed length is produced regardless of the lengths of input data. The length of hash value depends on the type of cryptographic hash function used. Although two different input data can, theoretically, have same hash value, calculation of this is infeasible for computers with computing capacity currently available. So, we can say that two data can be identical only if each of those data’s hash values is identical. Moreover, finding the input data from hash value of that data is infeasible.

Hash value of parent block is contained in the block header of the current block. A block in a blockchain has only one parent block. The first block, known as genesis block, does not contain parent block. Fig. 2 illustrates a continuous chain of blocks in a blockchain.
**Fig. 2** A continuous chain of blocks in blockchain

**Block**: A block is fundamental part of the blockchain which holds data in the blockchain. A block comprises a **block header** and a **block body**. Fig. 3 illustrates a block.

**Fig. 3** A block in a blockchain

Block header consists of block version, merkle tree root hash, timestamp, parent block’s hash, nbits and nonce. Block version provides information to software system about the set of rules it should follow for validating the block. Block header contains single hash value of all the transactions (in case of crypto currency) computed using merkle tree. Timestamp in the block header provides current time as number of seconds passed since January 1, 1970. Block header also has hash value of its parent block. nbits is the encoded form of target threshold which the block header hash should not exceed for the block to be authentic.Nonce is random number added to the block by miner which is increased until the value of block’s hash having required number of leading zero bits is obtained.

Block body can contain any data. In case of crypto currency, transaction counter and transactions are contained.
in the block body\textsuperscript{11}.

\textit{Working mechanism of blockchain:}

We will explain the working mechanism of blockchain by describing how Bitcoin works. Nodes in a blockchain network form a peer to peer network and have a pair of public and private keys. They use these keys for interaction in the network. Public key is used as the node’s identity in the network and private key is used to digitally sign transactions\textsuperscript{2}. Asymmetric cryptography is used for digital signature\textsuperscript{11}. Transfer of value between two Bitcoin wallets is termed as a transaction. Private Key is a data unique to the owner of the wallet and is kept secret. It is used by the owner of wallet to sign transactions providing a mathematical proof that the transactions are actually done by himself/herself\textsuperscript{14}.

Once a transaction is signed by a node it is broadcasted all over the network. The transactions are then collected and appended in a proposed block for confirmation\textsuperscript{14}. Miner nodes add the proposed block to the blockchain through mining process. Blocks after being mined are added to the chain and are broadcasted back to nodes in the network. Nodes check validity of transactions (i.e. coins are double spent or not) contained in the newly formed block. If all the transactions are found valid, nodes check hash value of the block’s parent block in the block’s header and add the block to the chain next to its parent block and apply transactions contained in the block. This completes one round and it is a repeating process\textsuperscript{2}.

Double spending is a problem where previous owner of a particular coin transacts the coin back to him/her and transacts the same coin to another user without current owner’s consent\textsuperscript{15}. To make sure that a coin being transacted has not been double spent, nodes in the Bitcoin network have to be aware of all the transactions ever completed. In order to achieve this, there must be a record of chronological order of transactions the network agrees to. Only the first transaction done by a particular owner is considered valid and any later attempts by the same owner to double spend the coin is deemed invalid. As a solution to this problem, signed transactions are placed in block in the order in which they were received first\textsuperscript{13}. In a network where nodes do not trust each other, consensus has to be reached among the nodes on a particular order of blocks and transactions in it. Consensus algorithms come into play to obtain a chronological order of record agreed by majority of nodes in the network.

\textit{Proof of Work:} Bitcoin uses proof of work algorithm for reaching consensus in the network. In this consensus attaining mechanism, to add a block to blockchain, nodes in the network should spend their computational resources to find hash value of the block with required number of leading zeros by increasing nonce in it. This process is known as mining. SHA-256 hash function is used in Bitcoin. Every single node in the network can involve in mining. Once the required hash is obtained by any node, the block is added to the blockchain. The block, once included in the blockchain, cannot be removed without doing the computational work again. The average work required to be done by the miner is exponential to the number of leading zeros required in the hash value. In addition, blocks are time stamped to inform the network about the time at which transactions in the block were updated to the world. Time stamp also makes sure that the transactions in the block had existed at that time\textsuperscript{13}. The idea behind this algorithm is that a block on which work has been done is agreed upon by majority and becomes part of the blockchain. Transactions present in these blocks are only considered valid.

During mining process, a situation may arise where two miners mine two different blocks at the same time. In this situation, forks are formed and nodes in the network aren’t sure which block to accept as a part of the chain. A particular chronology of blocks cannot be maintained if forks aren’t resolved. To resolve the issue, nodes in the network reject shorter forks and only accept the longest chain available in the network as it is the
chain in which most work is done. During this, nodes work on the block which they receive first. In next round, it is improbable to extend chain of block in both forks at the same time again. When one fork becomes longer than the other, nodes working (mining) on the shorter fork reject it and start working on the longer one. In this way, single chain of blocks agreed by majority of nodes is maintained.

Some other consensus algorithms in use are:

**Proof of Stake:** Proof of stake (PoS) is an energy saving consensus algorithm compared to proof of work. PoS takes node’s stake (economic/coin age) into account. Thus, only nodes having stake can be a validator in the network. In this algorithm, a set of validators propose and vote on the next block to be created by taking turns. Weight of the validator’s vote depends on the validator’s stake. Ethereum’s Casper implementation uses PoS based on economic stake. To become a validator, user on Ethereum has to lock Ethereum’s currency ether as a deposit. To make the proposed block a part of the blockchain, validator votes on the particular block. At the end of the process, all validators agree on whether a particular block is accepted or discarded.

**Practical Byzantine Fault Tolerance:** Practical Byzantine Fault Tolerance (PBFT) algorithm provides solution to Byzantine faults-crashing or arbitrary behavior which can be observed in asynchronous environment. In this algorithm, a primary node is selected which can mine a block. The process is divided into three phases. A node has to receive more than two third of total votes from all other nodes in each phase to enter into next phase. Node which can progress to final phase and get two third of total votes becomes primary node. PBFT can tolerate adversary only if the number of faulty nodes is less than one third of the total number of nodes.

**Use of blockchain in addressing the problems faced by migrant laborers:**

Our solution consists of a software system which facilitates the employment contract procedures. The software can be divided into two parts as shown in fig. 4.

![Fig. 4 Two sections of the software system](image)

In frontend, a web/mobile based application which consists of an advertisement portal for advertisement
of approved job positions with all the details regarding the job is present. Prospective migrants can view vacancies for job positions, apply for job positions and sign electronic contracts with recruitment agency via the application using their unique identification account.

This ensures that prospective migrants have assessed a range of job positions and applied for the job which they find suitable. In addition, as these advertisements are posted by recruitment agencies, it allows prospective migrants to get contacted to recruitment agencies without the need of individual agents. Moreover, for migrants’ comfort, prospective migrants can easily be provided an option to view advertisements and job contracts in the language which they find comfortable.

**Unique account:**

For prospective migrants: Prospective migrant’s passport number is used for creating unique account for prospective migrants.

For recruitment agencies: Registration number of recruitment agency is used for their unique account. Unique accounts act as an identity of the migrant and recruitment agency in the system. They use it to cryptographically sign labor contracts.

**Procedure for obtaining labor permit in new system:**

Prospective migrant contacts the recruitment agency that is recruiting workers for the job, which the migrant is interested in. If selected by the recruitment agency, prospective migrant fulfills the requirements of obtaining labor permission: undertake skill oriented trainings for their job, attend pre-departure orientation training, undergo full medical examination, buy life insurance, pay required amount to Foreign Employment Welfare Fund and obtain work visa of the destination country. Electronic contract containing details of the job is then cryptographically signed between the recruitment agency and the migrant via the web/mobile application. Required documents (proof of undertaking of required trainings, medical examination, life insurance, bill stating payment made to the welfare fund and valid work visa) and the signed contract is forwarded to government officials for approval. Upon receiving all documents and the signed contract, government official requests prospective migrant to receive signed contract between the migrant and the foreign employer from the recruitment agency and present it to the government official. If no issue is found upon checking all the documents, worker is asked to pay recruitment fees to the recruitment agency. Hash value of the contract signed between worker and recruitment agency is included in a new block proposed to be a part of blockchain. This blockchain is a ledger of hashes of contracts and is maintained by Department of Foreign Employment (DOFE). Once enough number of hashes has been added which meets size limit of the proposed block, the block is included in the blockchain by DOFE. Only DOFE will have authority of including new block in the blockchain. Access to reading and storing the data in the blockchain is provided to all nodes (recruitment agencies, migrant workers, DOFE, etc.) in the network. Original contract is stored in cloud and can be accessed anytime via the web/mobile application. Address of hash in the block is included in the original contract to maintain a link between original contract and its hash in the blockchain. Duty of checking and approval of the documents required for obtaining the permit can be decentralized to district level for completing the process faster i.e. government official of prospective migrant’s home district checks and approves the required documents of that migrant. Once hash of a contract is included in the blockchain, removing that record and replacing it with new one becomes infeasible for fraudulent recruiters. Ledger of hashes of contract will be stored in every node. Replacing data in only one node would be of no use. Due to blockchain’s feature, replacing a single contract would require replacing the block which contains hash of that particular contract and subsequent blocks in the blockchain after it with a new one – which is infeasible as only DOFE has authority to make changes in the blockchain.
Thus, this system leaves no room for contract substitution from fraudulent recruiters. It enables signed contracts to be a permanent record. This creates single source of truth of contract status and its history. This system will also regulate recruitment agencies as only registered recruitment agencies will have unique account to recruit workers using this system.

Original contracts can be verified at anytime by producing a hash and matching it with the one in blockchain. Verified contract can be used as evidentiary documents for seeking redress and compensation if terms and conditions are not met.

Conclusion and Future work:

Nepalese laborers in foreign employment have been facing frauds related to contract substitution, misrepresentation of terms and conditions. These problems have left the laborers vulnerable to exploitation. This paper proposed and analyzed a software system based on blockchain technology which aims to solve these problems by regulating labor recruitment and permit procedure and making the process accessible, robust, transparent, organized and safe. This system also regulates recruitment agencies and ensures good governance in foreign employment management.

In future, study could be carried out to explore ways to implement this system for those migrants who are already working overseas and willing to renew their labor permits. The system described on this paper only deals with regulating labor permit procedure for prospective migrants.

Acknowledgement

We would like to acknowledge St. Xavier’s College, Maitighar for providing financial support to give shape to this paper. We are also thankful to Mr. Dinesh Lohani for reviewing the draft and giving constructive comments.

References

1. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is Current Research on Blockchain Technology? - A Systematic Review,” *PLoS ONE*, vol. 11, no. 10, p. e0163477, doi:10.1371/journal.pone.0163477, (2016).
2. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, (2016).
3. Ministry of Labour and Employment, “Labour Migration for Employment | A Status Report for Nepal: 2015/2016/2016/2017,” (2018).
4. International Labour Organization, “PROMOTING INFORMED POLICY DIALOGUE ON MIGRATION, REMITTANCE AND DEVELOPMENT IN NEPAL,” (2016).
5. S. M. Liu, “Exploitation of Overseas Migrant Labor: Analysis of Migration Policy in Nepal and the Philippines,” *University of Pennsylvania Scholarly Commons*, (2015).
6. B. Farbenblum, S. Paoletti, E. Taylor-Nicholson, and B. Sijapati, “Migrant Workers’ Access to Justice at Home: Nepal,” *Migrant Workers’ Access to Justice Series*, (2014).
7. Investopedia, “Blockchain Definition | Investopedia,” [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: 28-Jun-2018].
8. B. A. Tama, B. J. Kweka, Y. Park, and K. H. Rhee, “A Critical Review of Blockchain and Its Current Applications,” in *Proceedings of 2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, no. August, pp. 109–113 (2017).
9. T. Fisher, “What Is a Cryptographic Hash Function?,” [Online]. Available: https://www.lifewire.com/
cryptographic-hash-function-2625832. [Accessed: 29-Jun-2018].

10. H. L. Su, “What Is A Cryptographic Hash?,” [Online]. Available: http://homeowmorphism.com/articles/17/What-Is-A-Cryptographic-Hash#collision-resistance. [Accessed: 01-Jul-2018].

11. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in Proceedings of 2017 IEEE 6th International Congress on Big Data, no. October, pp. 557–564 (2017).

12. Bitcoin, “nBits, Target Threshold - Bitcoin Glossary,” [Online]. Available: https://bitcoin.org/en/glossary/nbits. [Accessed: 02-Jul-2018].

13. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” URL: http://www.bitcoin.org/bitcoin.pdf, (2008).

14. Bitcoin, “How does Bitcoin work? – Bitcoin,” [Online]. Available: https://bitcoin.org/en/how-it-works. [Accessed: 23-Jul-2018].

15. M. Rosenfeld, “Analysis of hashrate-based double-spending,” pp. 1–13, (2014).

16. “Proof of Stake FAQs,” [Online]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs. [Accessed: 01-Oct-2018].

17. S. King and S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” Self-Published Paper, August, vol. 19, (2012).