Block Chain Review in the Educational System

Hiren Kumar Praharaj, Sonali Pradhan
College of Engineering Bhubaneswar, Biju pattnaik University of Technology, Odisha, India

ABSTRACT: The Blockchain is scattering its impact beyond the field of digital currency to further areas. Also in education, Blockchain can be the transformational power in education as well. In this review paper we will analyze the main problems that occur from storing the educational records in block chain and therole of blockchain technology in Education System instead of financial currencies .The platform is considered to act as a decentralized ledger, with special concern for privacy and mechanisms of data acknowledgment. The block chain technology is absolutely affecting and could impact the education system and education technology in a more effective way. Blockchaintechnology can succeed this outstanding achievement rapidly and internationally, with no central authority to administrate. Every countries, the field of education is a central focus is like a backbone of human beieng, so that the future of other important areas, including science, medicine, agriculture, industry and almost all others, is dependent on the country's education levels.

KEYWORDS- Blockchain, decentralized ledger, Internet of things, security.

I. INTRODUCTION

Nowadays, crypto currency has become a buzzword in both Industry and universities As one of the most successful crypto currencies, Bitcoin has great success with its capital market that reaches 10 billion dollars in 2016 [1]with a specially designed data storage structure, bit coin transactions ,the network could happen without third parties and the core.The technology to build Bitcoin is blockchain, which was the first proposal in 2008 and implemented in 2009 by Santoshi Nakamoto [2].It could be considered a public accounting book and everything is busy

Transactions are stored in a list of blocks. This chain grows as new blocks are added continuously. Asymmetrical they have been encrypted and distributed consensus algorithms implemented for the user's security and the consistency of the ledger. The Blockchain technology generally has key features of Decentralization, Persistence, Anonymity and Verifiability, with these features, block chain, can greatly save costs and improve the efficiency ,since it allows you to make payment without any kind of bank or any intermediary, blockchain can be used in more services such as digital resources, remittances and online payments.[3]. Furthermore, it can also be applied in other fields, including smart contracts [16], public services , Internet of Things (IoT) , reputation systems and security services. If we talking about the the crypto currency exchanges, which have made crypto currencies more accessible.

While it is easier to use crypto currencies today, it still takes a degree of technical knowledge: Private keys, public keys,hashed wallet addresses, syncing, nodes, are some of the terms new users have to familiarize themselves with. These are obstacles to adoption that have undoubtedly hindered the adoption of crypto currencies by the masses. We believe that what is necessary to make the adoption of crypto currency a reality in the mass market is to make the whole experience easy and familiar.

All the technical details of the underlying protocols should be abstracted by the average user so that the use of crypto currency is as natural as the use of any social networking platform. While other blockchain projects are working to solve the problem, we believe this is a small part of the problem. Other projects are also working on the creation of crypto currency. Again, this is only part of the problem. It is the only platform that addresses mass adoption and end users to companies. This will provide solutions that can be used by both end users and merchants in daily crypto currency transactions.

The massive adoption of the crypto currency can not wait two or three years,this must happen now. Therefore, with Tip, we are working on this as our main objective and we are offering a solution that solves the problems described immediately ,but in this paper we focuses on the role of blockchain technology in Education System instead of financial currencies. Before that let understand the more about the blockchain,Some of these documents are detailed below. Part-IIntroduction. Part-II begins with the construction of the blockchain (Architechture).Part-III Blockchain in educational sector Part-IV the characteristics of blockchain. Part-V Characteristics of Block Chain –Comparison Part-VI concludes the paper.

II. BLOCKCHAIN ARCHITECTURE

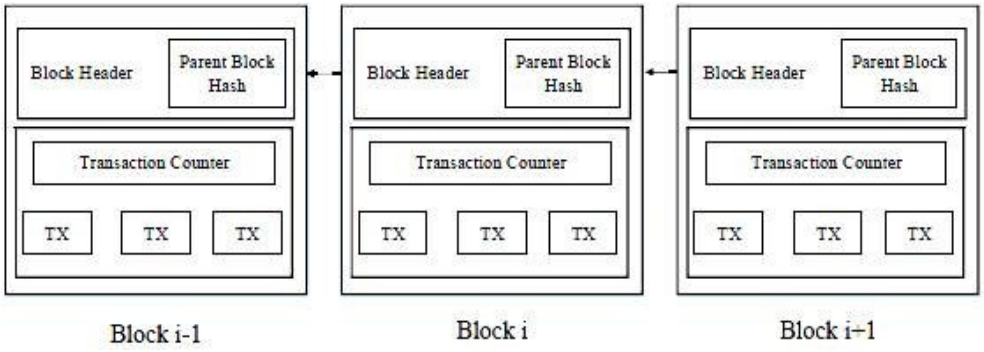

Fig. 1.1: An example of blockchain which consists of a continuous sequence of blocks.

Blockchain is a sequence of blocks, which contains a complete List of transaction records as a normal public record[14] Figure 1.1 shows an example of a blockchain.With a hash of the previous block contained in the block header, a block It has a single parent block. The hashes have also been memorized (the children of the ancestors of the block) in the chain of ethereum blocks [15]. The first block of a blockchain,It's called a genetic block that does not have a main block.

(A) Block

block contains the block header and the block body as shown in Figure 1.2. The block header contains:

(i) Block version: identify which set of block validation rules to follow.

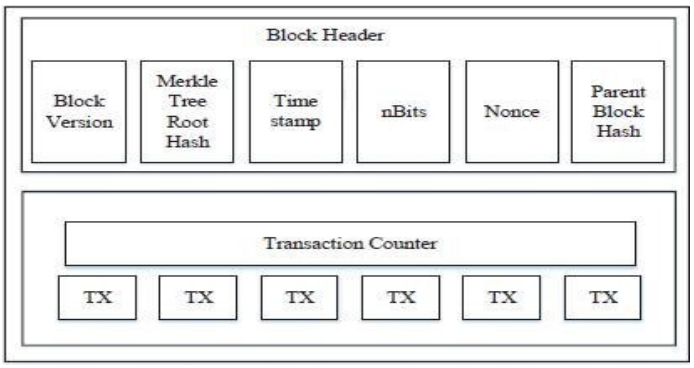

Fig 1.2 Block Structure

(iii n Bits: target beginning of a valid block hash
(iv) Root Hash of the Merkle tree: the hash value of all transactions in the block
(iv)Timestamp: current time as seconds in universal time from 1 January 1970.
(v) Nonce: a four byte of field, which generally begins with 0 and increases 4 each hash calculation.
(vi) Parent Block Hash: hash value of the previous block which is a 256-bit that points to the previous block.
vi) Transaction counter: consists of a transaction and the extreme number of transactions that a block can enclose depends on the size of the block and the size of each transaction.[16].

(B) Digital signature

Each user has a private and public key pair. The private key that will be kept confidential is used to sign transactions. The basically digital signature is involved in two phases: first is signature phase and second is verification phase. For example, an A1user wants to send a message to another B1 user. (1) In the signing phase, A1 encrypts their data with own private key and sends B1,the encrypted result and the original data. (2) In the verification phase, Bob validates the value with Alice's public key. In this way, B1 could easily check whether the data was tampered with or not. The typical digital signature algorithm used in blockchains is the digital signature algorithm of the elliptic curve (ECDSA) [16].

(C) Key Features Of The Blockchain

Blockchain has the following key features.
• **Decentralization.** In the centralized transaction systems, each transaction must be validated through the central trust organization (for e.g. the central bank), which necessarily translates into cost and performance bottlenecks in the central servers. In contrast to centralized mode, a third blockchain part is no longer needed. Blockchain Consensus algorithms are used to preserve data uniformity in the distributed network.
• **Persistence** Transactions can be authorised quickly and invalid transactions will not be accepted by honest miners. It is almost unbearable to delete or restore transactions once they are included in the block chain. Blocks containing invalid transactions can be discovered immediately.
• **Privacy.** Every single user can interact with the chain of blocks with a generated address, which does not expose the true identity of the user. The blockchain can not guarantee the perfect protection of privacy due to fundamental restrictions.

III. BLOCKCHAIN IN EDUCATIONAL SECTOR

In all the developed countries of the world, the field of education is a central objective. This is because the future of other important sectors, such as science, medicine, agriculture, industry and almost all others, depends on the levels of education in the country. Despite the remarkable developments in robotics and Internet and IT technologies, human resources remain the most valuable resource four almost all companies. Contrary to general opinion, progressive technologies help to improve the domain of personnel training and solve many problems. Not only private institutes but also many state educational institutions are preparing to implement blockchain-based tools or are conducting research that will identify the strong point and weaknesses of the implementation of blockchain technology in education. Let's review the problems that are faced in the field of education, ways to solve them through blockchain technology and examples of perspectives on the implementation of blockchain technology in this field.

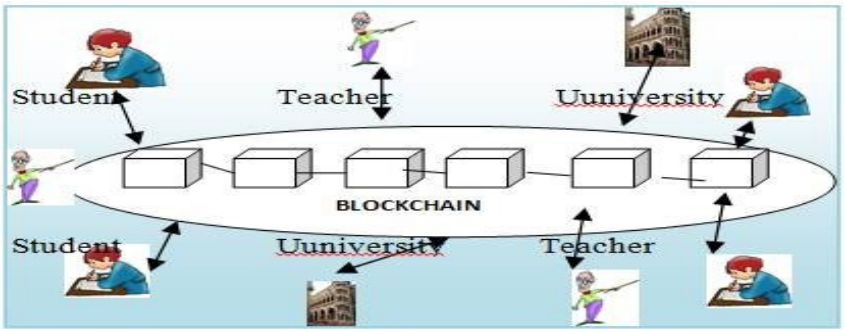

Fig3.1:BlockChainCommunication in Education

IV. STUDY OF EDUCATION SYSTEM

The education addresses major challenges that go beyond the simple optimisation of the teaching-learning processes (Bartolome, 2011, Bartolome and Grané, 2013) and respond to the changes produced by technologies to knowledge that, depending on the state of the Frankenstein Syndrome (Postman , 1991), not only change our habits, but also our way of thinking. Now, can blockchain technology provide a solution to some of the problems that arise from these changes? Let's try to analyse two cases in detail. Learning is no longer an activity that takes place during an initial period of formal modality and is enriched by experience in professional and vital practise. Lifelong learning has become a need four work (Longworth, 2005), according to the mode of human learning (Bruer, 1999), a requirement of 21st century citizenship (Martin Ortega, 2008), which concerns both the social framework in what we move and biographical social learning (Alheit&Dausien,2002). However, although this solution facilitates the transfer of students between institutions and the transfer of reliable information to employers, there has been no progress in the guarantee of content (skills and abilities), whose validation remains centralised in institutions with a reputation also ratified by national or transnational authorities. The questionnaire is asked to be a record of the itinerary that a student will follow in their learning and knowledge

V. LITERATURE REVIEW

Characteristics of Block Chain –Comparison

Even though the blockchain technology can be observed as an developed technology and thus still has room for enhancement in terms of efficiency and technical aspects [12], its underlying features can already be discussed. To evaluate these features in a structured and systematic manner, the identified peer-reviewed articles and the respectively mentioned attributes are presented in the concept matrix in Table 1.

Our analysis shows that blockchain technology conveys to bear a diversity of features, which are, in the following, analyzed concerning their interrelations, deriving a set of key features. For example, it is supposed that the features “shared and public” as well as “low resistance” lead to increased transparency in a system, since information is made publicly available among applicants without being influenced by a third party. Two major features are to be recognised when looking at blockchain technology, namely its trust inducing and decentralized nature.

Since blockchain technology can be considered an emerging technology and, therefore, still has room four improvement in terms of efficiency and technical aspects [12], its basic characteristics can already be discussed. To evaluate these characteristics in a structured and systematic way, the identified articles reviewed by pairs and the attributes mentioned are presented in the conceptual matrix in Table 1.

Our analysis shows that the blockchain technology has a variety of characteristics, which are, in Next, we analyse in relation to their interrelations, deriving a set of key characteristics. Four example, it is assumed that the "shared and public" and "low friction" characteristics lead to greater transparency in a system, since the information is made available to the public among the participants without being influenced by a third party.

Two main characteristics must be identified when observing blockchain technology, that is to say its evocative and decentralized nature ,because blockchain technology is based on a peer-to-peer network [9], which is combined with the ability of technology to protect interactions between two people through the use of public-key cryptography and the fact that identities are covered from pseudonyms, a high degree of privacy is enabled four its participants [3]. Reliability within the system is established by the use of two factors. On the one hand, the information of the transactionis shared and stored through the network and, therefore, it is treated redundantly [2] and, on the other hand, because the technology is based on data and codes, it facilitates the introduction of automated measures, which in turn can reduce individual errors since there is little need four manual intervention [4]. By allowing its participants to integrate their own programmes, develop and distribute their own code, thus modelling their environment, blockchain technology facilitates the creation of an open and versatile system [4].

A popular example of this feature is the so-called smart contract, which is a piece of code that acts as a contractual agreement between two parties [2]. While some authors explicitly mention the notion of the "reliable" technology of the block chain, others describe it indirectly and also through a public and shared vision of the transactions that occur in the network as equals; that guarantees integrity Datain the blockchainUsingblockchain technology enables its participants to establish a shared and publicly unfolded relationship. Given that there is a shared vision of all past and current transactions, participants have complete information about the activities of the system [3]. New transactions are transmitted throughout the network and, since there is no single intermediary that controls the system, users can interact directly, which reduces friction [2].Trust can also be simplified through the essential characteristic of technology to guarantee the integrity of the data, which is stored in the database itself, since direct interaction is guaranteed through public-key cryptography and the fact that that through its transparent nature the user can verify the transactions transmitted on the basis of predefined rules [1].

Another factor that helps generate trust is the immutable design of the database, which means that once a transaction has been added to a block, which in turn is added to the block chain, this transaction can not be change [7]. This process is facilitated through the application of the so-called consensus mechanism, which for example request the calculation of a work test.A work test(poof-of-work) can be considered as a computational puzzle, which requires a lot of effort to be solved, but whose solution is easily verifiable by others. In the event that a user finds the solution, it is shared with the remaining participants in the network, which in turn can verify their correctness, thus obtaining a consensus on the solution.

A crucial aspect of the job test is that the puzzle a user is solving depends on the previously accepted and agreed blocks ofthe blockchain. As a series of participants is attempting to form and add new blocks to the block chain, changes in the block chain would result in variable solutions, revealing incorrect use or manipulation [9]. Both trust and decentralization are closely related and interrelated in the case of blockchain technology.

On the one hand, the mechanisms used to establish trust, such as transparency, integrity and immutability of data, are necessary for the creation of a decentralized network, where reliable and reliable transactions can be made without a reliable third party.On the other hand, decentralization provides the meanings for consensus building and leaves the need for a trusted third party obsolete.

Characteristics							
Author(s)	Trust	Shared and public	Low friction	Peer verification	Cryptography	mutability	Decentralization
Barber et al. [1]	✓		✓	✓		✓	✓
Beck et al. [2]	✓	✓	✓	✓	✓	✓	✓
Böhme et al. [3]		✓			✓	✓	✓
Bonneau et al. [4]	✓		✓				✓
Cai and Zhu [5]	✓	✓		✓	✓	✓	
Cucurull and Puiggali [6]	✓	✓		✓	✓	✓	✓
Delmolino et al. [7]	✓	✓		✓	✓		
Eyal et al. [8]	✓	✓	✓		✓	✓	
Garay et al. [9]	✓	✓	✓	✓			✓
Garman et al. [10]	✓	✓			✓	✓	✓
Gerstl [11]	✓	✓	✓	✓	✓	✓	✓

Table 1: Characteristics Analysis of Block Chain

VI. CONCLUSION

The Blockchain technology has a positive influence and could influence the education system and educational technology more effectively. Blockchain can carry out this exceptional coup d'etat quickly and internationally, without any central authority being governed. In summary, blockchain is a type of falsification-proof data structure and tracks digital assets as they pass from one owner to another. The digital quality could be a digital currency like Bitcoin, any certificate or transaction could be a monetary transaction between anonymous strangers on the Internet. BLockchain has demonstrated its potential to transform the traditional industry with its key features: decentralization , persistence, privacy and audit capacity.

In this paper, we explain the brief description of the blockchain. First, we offer a general description of the blockchain technologies, which include the architecture and the key features of blockchain.After that we discuss the role of blockchain in the education sector. We have analysed and compared the characteristics of the blockchain in different aspects. Currently, blockchain-based applications are leaping and we alsoplan to carry out exhaustive research on blockchain-based applications in the future.

REFERENCES

[1] Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better - how to make bitcoin a better currency. In: Keromytis, A.D. (ed.) Financial Cryptography and Data Security: 16th International Conference, FC 2012, pp. 399–414. Springer, Heidelberg (2012)

[2] Beck, R., StenumCzepluch, J., Lollike, N., Malone, S.: Blockchain - the gateway to trust-free cryptographic transactions. In: Twenty-Fourth European Conference on Information Systems (ECIS), pp. 1–14 (2016)

[3] Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: economics, technology, and governance. J. Econ. Perspect. 29, 213–238 (2015)

[4] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy, pp. 104–121 (2015)

[5] Cai, Y., Zhu, D.: Fraud detections for online businesses: a perspective from blockchain technology. Financ. Innov. 2, 20 (2016)

[6] Cucurull, J., Puiggalí, J.: Distributed immutabilization of secure logs. In: Barthe, G., Markatos, E., Samarati, P. (eds.) STM 2016. LNCS, vol. 9871, pp. 122–137. Springer, Cham (2016). doi:10.1007/978-3-319-46598-2_9

[7] Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E.: Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: Clark, J., Meiklejohn, S., Ryan, P.Y.A., Wallach, D., Brenner, M., Rohloff, K. (eds.) FC 2016. LNCS, vol. 9604, pp. 79–94. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53357-4_6

[8] Eyal, I., Gencer, A.E., Sirer, E.G., van Renesse, R.: Bitcoin-NG: a scalable blockchain protocol. In: Proceeding of 13th USENIX Symposium Networked Systems Design and Implementation (NSDI 2016), pp. 45–59 (2016)

[9] Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: analysis and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 281–310. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46803-6_10

[10] Garman, C., Green, M., Miers, I.: Decentralized anonymous credentials. In: Network and Distributed System Security (NDSS) Symposium 2014, pp. 23–26 (2014)

[11] Gerstl, David S.: Leveraging bitcoin blockchain technology to modernize security perfection under the uniform commercial code. In: Maglyas, A., Lamprecht, A.-L. (eds.) Software Business. LNBIP, vol. 240, pp. 109–123. Springer, Cham (2016). doi:10.1007/978-3-319- 40515-5_8

[12] D. Lee KuoChuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc: eee:monogr:9780128021170

[13] V. Buterin, "A next-generation smart contract and decentralized appli-cation platform," white paper, 2014.

[14] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001

[15] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[16] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.