Blockchain Architecture to Higher Education Systems

K. Palanivel
Computer Centre, Pondicherry University, India

Abstract:-**The blockchain is an emerging technology that serves as an immutable ledger, which allows transactions to take place in a decentralized manner. It has become a publicly available infrastructure for building decentralized applications and achieving interoperability. Blockchain-based applications ensure transparency and trust between all parties involved in the interaction. The blockchain also makes blockchain technology-based services interest to the education sector. Nowadays, educational organizations focus on online education and propose to create a system based on educational smart contracts in a public ledger. This public ledger will be shared between major offline educational institutes around the world. From a software architecture perspective, blockchain enables new forms of distributed software architectures across a large network of untrusted participants. The objective of this article is to apply blockchain technology in learning solutions and to propose a blockchain architecture to e-Learning solutions in Higher Education Systems. The proposed architecture exploits the benefits of the blockchain and offering security, anonymity, longevity, integrity, transparency, immutability and global ecosystem simplification, in order to create a globally trusted higher education credit system.**

Keywords **– Blockchain, blockchain model, blockchain architecture, higher education institutions, e-learning solutions**

I. INTRODUCTION

The blockchain is an emerging technology[15], which provide significant opportunities to disrupt traditional products and services due to the distributed and decentralized in nature. The features such as the permanence of the blockchain record and the ability to run smart contractsmake blockchain technology-based products or services significantly different from previous internet-based commercial developments and of particular interest to the education sector. In addition, currently, stakeholders within education are largely unaware of the social advantages and potential of blockchain technology.

The increased interest and the variety of blockchain technologies lead to the growth of their application domains. The idea of storing educational records in the blockchain has been circulating in the press and academic papers for several years. Nowadays, most of the educational organizations focus on online education. These educational organizations propose to create a system based on the educational smart contracts in a public ledger. This public ledger can be shared between major offline educational institutes.

Blockchain technology is forecast to disrupt any field of activity that is founded on time-stamped record-keeping of titles of ownership. Within education, activities likely to be disrupted by blockchain technology include the award of qualifications, licensing and accreditation, management of student records, intellectual property management and payments. In education systems [25] student records are endless, and with blockchain technology, assets like attendance, courses, payments toward tuition if they attend a private school, grades, coursework, and even their diploma can become part of their personal blockchain record. Since these records cannot be deleted, this helps with data security in that it is immutable. It also belongs to the student, rather than to the school. With blockchain, no participant can tamper with a record after it has been saved. If a record has an error, a new record must be added to correct it, and both the incorrect and correct records will remain visible.

1.1Challenges in Present Education System

As of today, the standard process of education sector examinations has become very slow which causes uneven delays in the grading process [3]. When everything from sending copies to finalizing results is handled manually, it is not just expensive and time-consuming, but also causes a discrepancy in results, which is just not fair. At some places where still paperwork is involved, things get even worse.

1.2 Motivation Example

Employees in the education sector misplace essential papers now and then, and they include students who lose their diplomas at the most inopportune time. Then, there are students from war-torn areas intending to continue their education elsewhere, and students of a school whose server breaks down or the data completely wiped out, for some reason. The research question for this study iscritical to the shaping of a qualitative study.

- How to keep a reliable repository of academic records in a decentralized manner?
- How does a recruiter seamlessly verify certificates from educational institutes in a good amount of time?
- What is the best technology available that the learners can constantly upgrade their skills for professional and personal growth in the world today?

These and others who have trouble getting a copy of their school records can benefit from blockchain-encrypted credentials.Due to the nature of the platform, it has to operate on sensitive data, such as courses, assignments, solutions, payment, grades, certificates, etc. The motivation example is shown in Fig. 1.

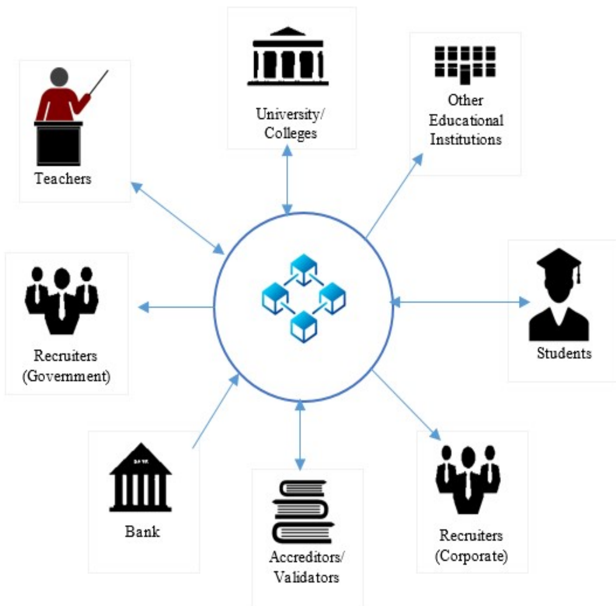

Fig.1 Motivation example for blockchain architecture

The blockchain in education [5] sector can help schools, colleges, universities to function in a streamlined manner by accessing candidate details from a shared database for verification purpose. Students can benefit from an easy certificate issuance process driven by smart contracts on completion of their course and establish self-sovereignty of their degrees and diplomas. Additionally, a student's stored e-portfolio on the blockchain can help accelerate processes in banks to verify candidature for an educational loan; and an employer to scrutinize the candidate's suitability for a position in his organization can access the very same e-portfolio.

The blockchain technology in the education sector can very well do wonders for the students and examination cell alike. Blockchain cannot only help in keeping the educational data safe and readily available but also cuts down the costs and saves time. With the use of blockchain, it aims to eradicate all the issues related to degree printing, verification and storage. Using advanced smart contracts, academic records will be transferred on the blockchain. It will enable educational institutes and e-learning platforms to issue certificates on the blockchain. Blockchain offers a number of benefits in streamlining the examination process. Some of the key benefits of Blockchain in the education sector are the elimination of bias, elimination of intermediaries and reduced costs and paperwork.

1.3 Solution

It is proposed a blockchain-based decentralized architecture for higher education learning solutions. This architecture is built on the distributed P2P network system. The proposed architecture called *proof of educational transcript system* (or PETS) is flexible, secure and resilient because of their storage capacity and resource sharing on a global scale. The PETS architecture transfers the higher education grading system from the analog and physical world into a globally efficient, simplified, ubiquitous version, based on the blockchain technology.

This paper is organized as follow: In *technical background section*, terminology and recent taxonomies for blockchain systems are discussed. A blockchain architecture for e-Learning Solutions is introduced in the *proposed system section*. Finally, in *conclusion, section*a conclusion is drawn and an outlook presented.

II. TECHNICAL BACKGROUND

This section presents on blockchain technology and the impact of blockchain technology in higher education institutions. It starts by formulating a definition for the basic concept, which is followed by a presentation of the technology's inherent characteristics.

Blockchain, technology is lauded as having the potential to transform the global economy due to its ability to increase transparency and trust. A blockchain is a distributed digital ledger of transactions, the contents of which are verified and agreed upon by a network of independent actors. Transactions are recorded in a series of blocks that gives a clear timeline of who did what and when. Blocks of information (time stamping of life events) are secured by complex algorithms that are hard to hack and cannot be manipulated. Therefore, it has a huge role to play in validating identity management, without the use of an independent third party.

A more wordy definition [6]: *The blockchain is a distributed database that provides an unalterable, (semi-)public record of digital transactions. Each block aggregates a time stamped batch of transactions to be included in the ledger. A cryptographic signature identifies each block. These blocks are all back-linked; that is, they refer to the signature of the previous block in the chain, and that chain can be traced all the way back to the very first block created. As such, the blockchain contains an un-editable record of all the transactions made.*

Since each block of transactions is cryptographically linked to the previous block, it is extraordinarily difficult to change data stored in a blockchain thus making it immutable. For a new piece of data to be added to the blockchain, the independent verifiers must come to a consensus about its validity. Therefore, blockchain has multiple layers of verification, which makes the platform tamper-proof and robust against any fraudulent activity. Nodes or computers connected to the blockchain network get updated version of the ledger as and when new transactions are made. The benefits of blockchain are now going beyond the world of finance into other industries, including education, where trust is essential.

2.1 Characteristics of Blockchain

The blockchain technology can provide a secure chain of custody for both digital and physical assets through its functional characteristics that facilitate transactions through trust, consensus, security, and smart contracts. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability.

- *Decentralization.* In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting in the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, the third party is no longer needed in the blockchain.
- *Persistency.* Transactions can be validated quickly and honest miners would not admit invalid transactions. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.
- *Anonymity.* Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user.
- *Auditability.* Bitcoin blockchain stores data about user balances based on the unspent transaction output (UTXO) model. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switches from unspent to spend. Therefore, transactions could be easily verified and tracked.

With the above traits, blockchain can greatly save cost and improve efficiency.

2.2 Types of Blockchain

Blockchain networks can be categorized based on their permission model, which determines who can maintain them (e.g., publish blocks). It can be permissionless and permissioned. If anyone can publish a new block, it is *permissionless*. If only particular users can publish blocks, it is *permissioned*. A permissioned blockchain network is like a corporate intranet that is controlled, while a permissionless blockchain network is like the public internet, where anyone can participate.

Permissionless Blockchain- Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority. Any blockchain network user within a permissionless blockchain network can read and write to the ledger. Permissioned blockchain networks are often deployed for a group of organizations and individuals typically referred to as a consortium.

PermissionedBlockchain-Permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority (centralized or decentralized). Permissioned blockchain may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals. They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals.

The blockchain systems can also be categorized into three types: *public blockchain, private blockchain* and *consortium blockchain*. In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process. A private blockchain is regarded as a centralized network since it is fully controlled by one organization. The consortium blockchain constructed by several organizations is partially decentralized since only a small portion of nodes would be selected to determine the consensus.

2.3 Components of Blockchain

Blockchain technology can seem complex. However, it can be simplified by examining each component individually. The main components [13] of blockchain are *cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers and blocks*.

Cryptographic Hash Functions - An important component of blockchain technology is the use of cryptographic hash functions for many operations. This component calculates a relatively unique output for an input of nearly any size (e.g., a file, text, or image). It allows individuals to independently take input data, hash that data, and derive the same result – proving that there was no change in the data.

Transactions - A transaction represents a transfer of the cryptocurrency between blockchain network users. Each block in a blockchain can contain zero or more transactions. A blockchain network user sends information to the blockchain network. The information sent may include the sender's address, sender's public key, a digital signature, transaction inputs and transaction outputs.

Asymmetric-Key Cryptography - Asymmetric-key cryptography uses a pair of keys: a public key and a private key. Asymmetric-key cryptography enables a trust relationship between users who do not know to each other, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions to remain public. In contrast, symmetric-key cryptography in which a single secret key is used to both encrypts and decrypt. The data is encrypted with symmetric key cryptography and then the symmetric-key is encrypted using asymmetric-key cryptography.

Addresses and Address Derivation -Blockchain networks make use of an address along with some additional data (e.g., version number and checksums). The blockchain implementations make use of addresses in a transaction. To generate an address, it creates a public key, applying a cryptographic hash function to it, and converting the hash to text. Addresses may act as the public-facing identifier and oftentimes an address will be converted into a QR code for easier use with mobile devices.

Ledgers - A ledger is a collection of transactions. In modern times, ledgers have been stored digitally, often in large databases owned and operated by a centralized trusted third party (i.e., the owner of the ledger) on behalf of a community of users. These ledgers can be implemented in a centralized or distributed fashion. There is growing interest in exploring having distributed ownership of the ledger. The growing interest in distributed ownership of ledgers is due to possible trust, security, and reliability concerns related to ledgers with centralized ownership.

Blocks - Blockchain network users submit candidate transactions to the blockchain network via software. The software sends these transactions to nodes (non-publishing full nodes as well as publishing nodes) within the blockchain network. The submitted transactions are then propagated to the other nodes in the network. Transactions are added to the blockchain when a publishing node publishes a block. A block contains a block header and block data. The block header contains metadata for this block. The block data contains a list of validated and authentic transactions, which have been submitted to the blockchain network. The other full nodes will check the validity and authenticity of all transactions in a published block.

Chaining Blocks - Blocks are chained together through each block containing the hash digest of the previous block's header. If a previously published block were changed, it would have a different hash. This, in turn, would cause all subsequent blocks to also have different hashes since they include the hash of the previous block. This makes it possible to easily detect and reject altered blocks.

2.4 Working Principle of Blockchain

A blockchain is a tamper-proof, shared digital ledger, which records transactions in either a public or a private network. As it is distributed to all participants in the network, the ledger makes a permanent record as *blocks*. Each computer on the network is known as a "node". Instead of relying on a third party, such as a financial institution, to mediate transactions, participants in a blockchain network use a consensus protocol to agree on ledger content, and cryptographic hashes and digital signatures to ensure the integrity of transactions [9]. The principles of working of blockchain technology are shown in Fig.2

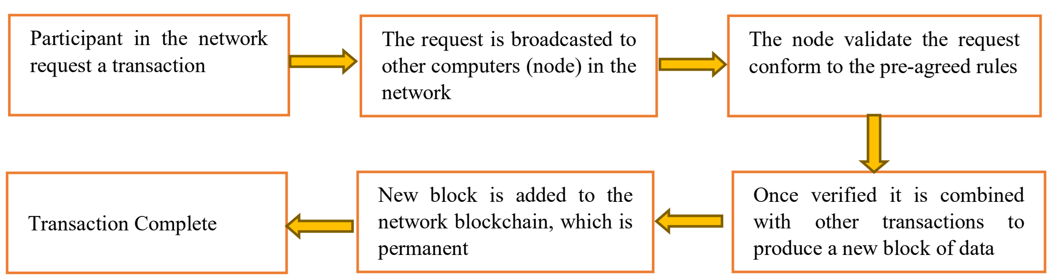

Fig.2 working principles of blockchain technology

The peer-to-peer blockchain network prevents any single participant or group of participants from controlling the underlying infrastructure or system. Participants in the network are all equal, adhering to the same protocols. At its core, the system records the chronological order of transactions with all agreeing to the validity of transactions using the chosen consensus model. The result is transactions that are irreversible and agreed to by all participants in the network.

2.5 Consensus Models of Blockchain

A key aspect of blockchain technology is determining which user publishes the next block. This is solved through implementing one of many possible consensus models. Blockchain technologies use consensus models to enable a group of mutually distrusting users to work together. There are several consensus models [4]as well as the most common conflict resolution approach are discussed.

Proof of work (PoW) consensus model - In this model, a user publishes the next block by being the first to solve a computationally intensive puzzle. The solution to this puzzle is the "proof" they have performed work. The puzzle is designed such that solving the puzzle is difficult but checking that a solution is valid is easy. This enables all other full nodes to easily validate any proposed next blocks, and any proposed block that did not satisfy the puzzle would be rejected. For example, Bitcoin, which uses the proof of work model, adjusts the puzzle difficulty every 2016 blocks to influence the block publication rate to be around once every ten minutes. This adjustment is to maintain the computational difficulty of the puzzle, and therefore maintain the core security mechanism of the Bitcoin network.

Proof of stake consensus (PoS) model– This PoS model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it. Proof of stake blockchain networks uses the amount of stake a user has as a determining factor for publishing new blocks. With this consensus model, there is no need to perform resource-intensive computations (involving time, electricity, and processing power) as found in proof of work. The methods for how the blockchain network uses the stake can vary are a *random selection of staked users*, *multi-round voting*, *coin ageing systems* and *delegate systems*. Regardless of the exact approach, users with more stake are more likely to publish new blocks.

Some permissioned blockchain networks use round-robin consensus model – This consensus model. Within this model of consensus, nodes take turns in creating blocks. This model ensures no one node creates the majority of the blocks. It benefits from a straightforward approach, lacks cryptographic puzzles, and has low power requirements. Since there is a need for trust amongst nodes, round robin does not work well in the permissionless blockchain networks used by most cryptocurrencies. This is because malicious nodes could continuously add additional nodes to increase their odds of publishing new blocks.

Proof of authority (Proof of Identity) consensus model– This consensus model relies on the partial trust of publishing nodes through their known link to real-world identities. The idea is that the publishing node is staking its identity/reputation to publish new blocks. Blockchain network users directly affect a publishing node's reputation based on the publishing node's behaviour. Publishing nodes can lose reputation by acting in a way that the blockchain network users disagree with, just as they can gain reputation by acting in a manner that the blockchain network users agree with. The lower the reputation, the less the likelihood of being able to publish a block. Therefore, it is in the interest of a publishing node to maintain a high reputation. This algorithm only applies to permissioned blockchain networks with high levels of trust.

Proof of elapsed time consensus model –In this (PoET) consensus model, each publishing node requests a wait time from a secure hardware time source within their computer system. Once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network, alerting the other nodes of the new block; any publishing node that is still idle will stop waiting, and the entire process starts over. After waiting the assigned time, the publishing node could request a signed certificate that the publishing node waited the randomly assigned time. The publishing node then publishes the certificate along with the block.

From a social perspective, blockchain technology offers significant possibilities beyond those currently available. In particular, moving records to the blockchain can allow for self-sovereignty, trust, transparency & provenance, immutability, disintermediation, and collaboration. Blockchain mechanism brings everyone to the highest degree of accountability. Therefore, solves the problem of manipulation. The data that belongs to us we can own it that is online identity and reputation will be decentralized. It provides durability, reliability, and longevity with the decentralized network. The data that are entered in blockchain-based systems are immutable which prevent against fraud through manipulating transactions and the history of data. Therefore, all the transactions can be investigated and audited easily.

Since blockchain technology is still new, many organizations are looking at ways to incorporate it into their businesses. The nature of the blockchain network has the potential to enable the development of a wide range of different applications [13] that are decentralized. Decentralized applications are becoming more and more important in recent years. Blockchain-based applications cannot be stopped censored or controlled and they ensure transparency and trust between all parties involved in the interaction. The use of decentralized application often depends on the context of the usage. Blockchain shows potential to be used in many different fields and some of them are domain registration, trading assets, cloud storage, voting, crowdfunding, car sharing, gambling and prediction markets, Internet of Things (IoT) and education.

2.6 Challenges in the Higher Education Sector

Education is the exchange of knowledge and skills through several channels. The process is more efficient if there is trust between all parties involved. This trust can play a crucial role in transforming higher education in the future. The blockchain technology has the potential to change the Higher Education Sector (HES) [8] for the better, through decentralization and immutability. Some of the challenges that affect the HES are fraud detection, universal academic credentials, smart contracts, decentralized classrooms and transparency of scholarships. Blockchain technology can provide solutions to the above challenges. A blockchain is an immutable ledger of records. Once the information has been entered and verified, it cannot be changed. Additionally, no one can append information on the blockchain without the approval of the network users.

According to Rachael Hartley, 2018, Education is a multifaceted sector where different systems need to adapt to prepare students for the jobs of tomorrow. Having a fool-proof system that records a student's academic history before and during a working life can not only help in battling dishonesty but can also help to tackle the issues of bespoke learning. This will ultimately give people the best chance of determining their education path and a successful future career.

It can allow workers to build up a secure, verifiable digital record of formal qualifications, experience and soft skills gained over their lifetime. In addition, by using a smart contract, blockchain applications could provide students with the ability to gain greater control over their individual education through offering flexible access to content and courses suggested based on previous successes or failures and attainment.

2.7 Blockchain in Education

Blockchain technology provides a simple and encrypted way of ensuring that a person is qualified and educated enough to fulfil the requirements for a position. They provide a plausible means of security for employers and employees to prove their credentials in certain areas. It would be easy for employers to authenticate this information. This can provide a more secure solution to teacher-readiness accountability in educational institutions. It can also ensure that teachers have taken appropriate classwork for the job they are taking on, or help teacher show they are qualified in various areas [1].

- The Blockchain technology will accelerate the end of a paper-based system for certificates. Any kinds of certificates issued by educational organizations can be permanently and reliably secured using blockchain technology.
- The blockchain technology allows users to be able to automatically verify the validity of certificates directly against the blockchain, without the need to contact the educational organization that originally issued them.
- The blockchain technology can also be applied to intellectual property management, for the tracking of first publication and citations, without the need for a central authority to manage these databases.
- The blockchain technology is applied to create data management structures where users have increased ownership and control over their own data could significantly reduce educational organizations' data management costs, as well as their exposure to liability resulting from data management issues.
- The blockchain technology is also found that blockchain-based cryptocurrencies are likely to be used to facilitate payments within educational institutions.

From the above, blockchain technology is considered for creating and promoting a label for 'open' educational records and only supports or adopts technologies in compliance with such a label. The main beneficiaries of the adoption of blockchain-based technologies in education are likely to be networks of educational organizations and learners. It suggests outreach to the educational networks to help them understand the benefits of technology, the incorporation of the principles behind the technology into digital competence education for learners.

III. METHODOLOGY

With an emerging technology such as blockchain, with almost daily industry announcements and posts on specialist media, the use of qualitative methods currently represents a pragmatic approach in engaging with the subject at a time when research on the subject is at an embryonic stage, and where case studies involving the blockchain and education are exploratory and / or pilot initiatives. This study is based on qualitative research methods, using desk research, literature review and case studies to generate evidence.

The research approach involves literature review and desk review [26]. The *literature review* of any published literature on applications of blockchain technology to education, non-financial applications of blockchain technology more generally and digital methods for storing, securing, sharing and verifying academic credentials. The *desk review* utilizing primary sources covering technical specifications of major blockchain implementations, in particular, Bitcoin, Ethereum, and technical specifications of products released by vendors offering products built on top of blockchain technology, as well as of their governing structure, operations and intellectual property arrangements.

3.1 Architectural Design

The design taxonomy [29] is intended to help software architects evaluate and compare blockchains, and to enable research into architectural decision-making frameworks for blockchain-based systems. The discussion of architectural design issues for blockchain-based systems has structured the level of decentralization, support for client storage and computation, blockchain infrastructural configuration, and other issues.

Decentralization devolves responsibility and capability from a central location or authority. The decentralized systems include permission-less public blockchains. The two options for decentralization are *permission* and *verification*. A blockchain may be permissioned in requiring that one or more authorities act as a gate for participation. The code for public blockchains can also be deployed on private networks. Permissioned blockchains may be more suitable in regulated industries. The execution environment of a blockchain is self-contained. It can only access information present in a transaction or transaction history, and the states of external systems are not directly accessible. To address this limitation, a *verification* role can be introduced.

The blockchains provide some unique properties - the amount of computational power and data storage space available on a blockchain network remains limited. In regards to cost efficiency, performance, and flexibility, major design decisions in using a blockchain include choosing what data, computation should be placed on-chain, and what should be kept off-chain.

3.2 Challenges in the Traditional Education

Some of the challenges in the traditional education system are *recordkeeping, badges, on the job training, continuous professional training, etc.* The solution to the above challenges is the use of blockchain technology in the education system. Blockchain by design is non-editable. With technology, learners are finding newer ways to do so without any fuss. The learners are realizing that smaller chunks of learning, acquired over a period of time works much better than a conventional credential driven certificate from the educational institutions.

- *For recordkeeping,* blockchain technology provides a secure repository of such records, time-stamped can be a big help for all stakeholders.
- Using blockchain, *badges* would be recorded and time stamped. Badges could subsequently be used for up-skilling and used as learning currency for progression.
- *Badges* can be used to keep a record of all *credentials* earned during a lifetime. Such credentials would be more valuable than the current practice of issuing certificates.
- For on the *job training*, blockchain technology could help centralize humongous data and validate the process and certification for such learners.
- For *continuous professional education*, the blockchain technology is used to seamlessly record fragmented data such as continuous learning's from multiple sources and stack this up in a repository.

Blockchain mechanism brings everyone to the highest degree of accountability. Therefore, solves the problem of manipulation. It provides durability, reliability, and longevity with the decentralized network. The data that are entered in blockchain-based systems are immutable. Therefore, all the transactions can be investigated and audited easily.

3.3 Literature Survey

By looking at the main concepts, it finds that innovation, decentralization and digital innovation is amongst the most common concepts found in the literature. However, by categorizing the concepts, it discovers the – technological features, innovation, decentralization and ecosystems themes mentioned in the literature about the blockchain technology. It should be noted that some of the concepts are present within one or more categories as these present ideas that fall outside one category. Hence, these will establish a foundation for further analysis of the topic.

Stefan K. Johansen, 2018 provided comprehensive and detailed documentation of the current technological and literary state of the Blockchain technology within Information Systems research. He outlined in detail what is required for the Blockchain technology to function as a technological enabler for innovation and the required factors for success. It is noted that the Blockchain technology in its current state still has a way to go before the technology will reach a state considered sufficient for mainstream adoption.

According to [27], blockchain technology was expected to revolutionize the way transactions are performed, thereby affecting a vast variety of potential areas of application. As blockchain technology was centred on a peer-to-peer network, enabling collaboration between different parties, the service system is chosen as a unit analysis to examine its potential contribution. They identified a set of characteristics that enable trust and decentralization, facilitating the formation and coordination of a service system.

Karim Sultan [19] presented an overview of blockchain technology, identified the blockchains key functional characteristics, built a formal definition, and offers a discussion and classification of current and emerging blockchain applications.

BitRice [7] aimed to create a future-oriented data storage and content sharing ecosystem featured by privacy, security, impartiality, decentralization, distribution and sharing. It will enable users to commercialize their spare storage space and digitalize the value of their original contents (photos, videos and files) by sharing, and therefore become a mature project with real-life applications seamlessly integrating smart hardware with blockchain technology.

Zhaoyang [29] gave a perspective on using Blockchain as a secure, distributed cyberinfrastructure for the future grid. Firstly, the basic principles of Blockchain and its state-of-the-art were introduced. Then, a Blockchain based smart grid cyber-physical infrastructure model is proposed. Afterwards, some promising application domains of Blockchain in future grids are presented. Following this, some potential challenges are discussed.

Karamitsos [18] aimed to present the Blockchain and smart contract for a specific domain, which is real estate. A detailed design of smart contract was presented and then a use case for renting residential and business buildings is examined.

Leonardo [20]developed an ontology that helps to identify and clarify in detail what are the concepts and structures revolving around this technology and built a continuum of blockchain architectural solutions, ranging from a classic centralized IT architecture to one completely distributed within a public ecosystem.

Alok Kumar Jain [2] the education industry is changing before our eyes. No longer solely the province of a centralized learning environment in either the physical or virtual worlds, education now occurs via peer-to-peer interactions, online and from anywhere on the planet. Educational providers, particularly in higher education, are struggling to harness digital technology as a tool for transformation.

Muhamed Turkanović [21] proposed a global higher education credit platform, named EduCTX. This platform was based on the concept of the European Credit Transfer and Accumulation System (ECTS). It constitutes a globally trusted, decentralized higher education credit, and grading system that can offer a globally unified viewpoint for students and higher education institutions (HEIs), as well as for other potential stakeholders, such as companies, institutions, and organizations. As a proof of concept, they presented a prototype implementation of the environment, based on the open-source Ark Blockchain Platform.

Ioannis Karamitsos 17] aimed to present the Blockchain and smart contract for a specific domain, which is real estate. A detailed design of smart contract was presented and then a use case for renting residential and business buildings is examined.

3.4 Purpose, Scope and Objectives

This above study investigates the feasibility, challenges, and benefits of blockchain technology architecture in education, with a focus on the application of the blockchain to formal and non-formal credentials. It needs to overcome challenges on many fronts where educational credentials are concerned.

This paper focuses on identifying all relevant literature, due to the novelty of the technology. With the identification of relevant literature, it will analyze and synthesize the results found in the literature in order to identify gaps and propose model and architecture for future research. A conclusion will be established to provide researchers with the main contributions of the paper. The primary objectives of the study are to:

1. provide an introduction to blockchain technology in education and the use of blockchain technology in education landscape;
2. determine if the technology is fit-for-purpose for the recording of academic achievements and HEIs should it be deployed as an open standard;
3. Identify opportunities and challenges for the take-up of blockchain technology in higher education institutions.
4. provide a generic architecture to academic institutions

This study is primarily aimed at policy-makers in HES, educators and researchers. It may also be of interest to a more general readership with an interest in emerging technology, and its deployment within a wider socio-economic context. The design analysis performed here may not be valid, relevant or rigorous enough since they are yet to be widely identified, used and studied for blockchain-based systems. However, it believes that the high-level qualitative approaches to support the indicative qualitative findings in our study.

IV. PROPOSED ARCHITECTURE

This section outlines the proposed architecture called PETS, a blockchain-based higher education learning solutions. Blockchain technology is a growing area of interest for educational institutions. The exploratory study addresses the value-decentralized ledgers; in particular, those based on blockchain technology may bring to stakeholders within the educational sector, with a particular focus on its potential for digital accreditation of personal and academic learning.

4.1 Blockchain Considerations

When deciding whether to utilize a blockchain, the designer must take into consideration of factors and determine if these factors limit one's ability to use a blockchain or a particular type of blockchain: data visibility, full transactional history, fake data input, tamper evident and tamper resistant, transactions per second, compliance, permissions, node diversity, etc.

The proposed solution makes use of blockchain technologies to authenticate consumers at digital identity providers. The contribution is to provide a distributed and interoperable architecture model for the higher education credit system, which addresses a globally unified viewpoint for students and institutions. Potential employers can benefit from the proposed system. The PETS architecture is envisioned for processing, managing and controlling the academic credits and resting on a globally distributed P2P network, where peers of the blockchain network are HEI and users of the platform are students and organizations (e.g. companies as potential employers).

4.2 Features

Nowadays, blockchain is a very powerful technology in education. The most important features of the proposed system using blockchain are discussed below:

- *Decentralized:* In the proposed system, no single person or group holds the authority of the overall network. While everybody in the network has the copy of the distributed ledger with him or her, no one can modify it on his or her own. This unique feature of blockchain allows transparency and security while giving power to users.

- *Peer-to-Peer (P2P) Network:* Blockchain uses P2P protocol, which allows all the network participants to hold an identical copy of transactions, enabling approval through a machine consensus. For example, if you wish to make any transaction from one part of the world to another, you can do that with blockchain all by yourself within a few seconds. Moreover, any interruptions or extra charges will not be deducted in the transfer.
- *Immutable:* The immutability property of a blockchain refers to the fact that any data once written on the blockchain cannot be changed. Once the data has been processed, it cannot be altered or changed. In case, if you try to change the data of one block, you will have to change the entire blockchain following it as each block stores the hash of its preceding block. Hence, the data stored in a blockchain is non-susceptible to alterations or hacker attacks due to immutability.
- *Tamper-Proof:* With the property of immutability embedded in blockchains, it becomes easier to detect tampering of any data. There are two key ways of detecting tampering namely, hashes and blocks. Each hash function associated with a block is unique. Any change in the data will lead to a change in the hash function. Since the hash function of one block is linked to next block, in order for a hacker to make any changes, he/she will have to change hashes of all the blocks after that block which is quite difficult to do.

4.3 Design Factors

Several considerations need to be evaluated when providing a blockchain solution in the education section. They are security, scalability, data sovereignty, resilience, etc.

- *Scalability:* In the proposed blockchain architecture, the number of transactions can be very large. Transformation and connectivity need to provide scalable messaging and scalable transformation of data in the cloud for these data flows.
- *Data Sovereignty:* The physical location in which data is stored may be regulated, with the regulations varying from place to place. As a result, any blockchain system must take into account data sovereignty rules and store and process data only in those locations permitted by the regulations.
- *Resilience:* Blockchain systems should not depend on one single component at any point and should tolerate the failure of a single component. Components in the blockchain provider should be made resilient with multiple instances of programs and cloud services allied with data replication and redundancy on multiple storage systems.
- *Security:* As more data about people, transactions, and operational decisions are collected, refined, and stored, the challenges related to information governance and security increase. A secure community process validates the security of the execution of transactions, enabling a foundation of trust and the robust processing of transactions.

4.4 Properties

The fundamental functional properties supported in blockchains are immutability, non-repudiation, integrity, transparency, and equal rights. If data is contained in a committed transaction, it will eventually become in practice *immutable*. The immutable chain of cryptographically signed historical transactions provides *non-repudiation* of the stored data. Cryptographic tools also support data *integrity*, the public access provides data *transparency*, and *equal rights* allow every participant the same ability to access and manipulate the blockchain.

A distributed consensus mechanism consists of the rules for validating and broadcasting transactions and blocks, resolving conflicts, and the incentive scheme. The consensus ensures all stored transactions are valid, and that each valid transaction is added only once.

- *Trust* in the blockchain is achieved from the interactions between nodes within the network. The participants of the blockchain network rely on the blockchain network itself rather than relying on trusted third-party organizations to facilitate transactions.
- *Data privacy* and *scalability* are non-functional properties of public blockchains. The setting of privacy is limited. There are no privileged users, and every participant can join the network to access all the information on blockchain and validate new transactions.

There are scalability limits on the size of the data on the blockchain, the transaction-processing rate, and the latency of data transmission.

4.5 Platform View

The education process from the platform's perspective is as follows:

1. A student chooses an educational organization and a course that she wants to enrol in.
2. If the course is offered on a paid basis, the student uses the education app to pay the fee.
3. The educational organizations then verify the payment in the public ledger.

4. During the course, the educational organizations provide assignments and conduct exams that the student has to complete in order to get the score.
5. The student acquires the assignment, completes it and sends the signed solution back to the educational organizations.
6. The educational organizations then store the solution locally, grades, certificate, and transfers the score with the hash of the solution to the blockchain.
7. Upon the completion of the course, the student acquires a final score and this final score is added to the educational organization's chain.
8. The Recruiters can verify the score and certificate added in the public ledger.

4.6 Proposed Model

It is proposed to introduce proof of educational transcript system (PETS). In this model, the PETS application model will connect educational institutions into a single educational blockchain network of credits earned by learners/students. They will be able to choose courses and instructors from a pool of institutions, collecting the credits over a lifetime, and 'cashing them in' when they are degree-ready and the issuing institution agrees. PETS is an educational blockchain actual tool to ensure it.Fig.3. shows the various actors in the proposed proof of educational transcript system model.

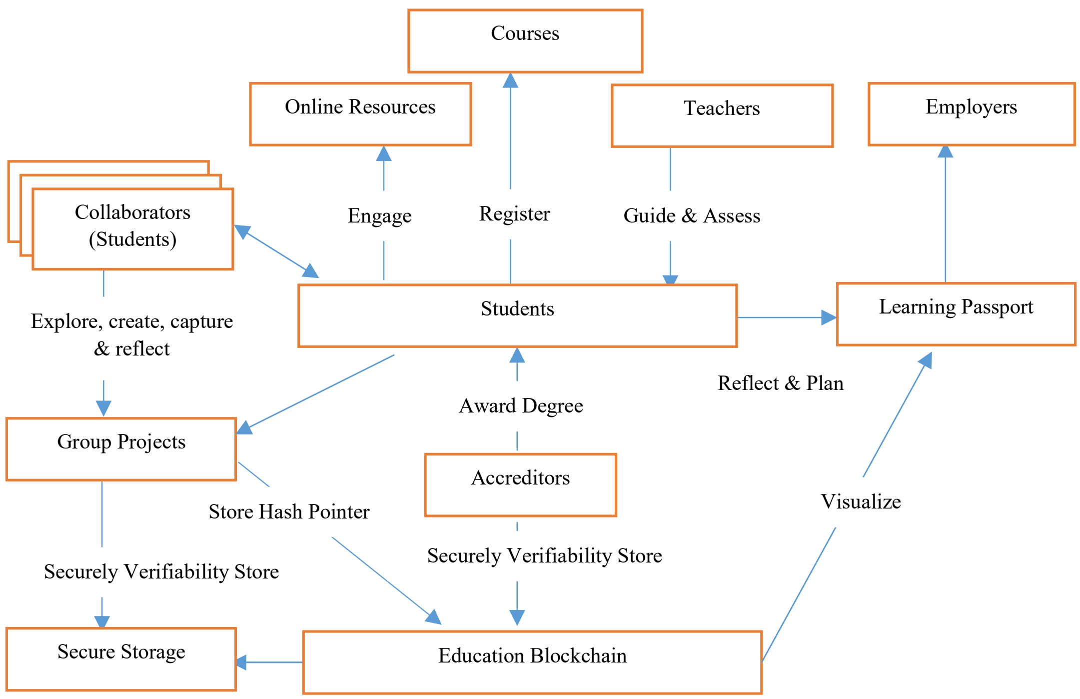

Fig 3. Actors in the proposed PETS model.

4.7 Proposed Architecture Model

The PETS architecture contains private chain which consists of sensitive dataand public chain which, the information necessary to validate the integrity and authenticity of the private blocks. The key entities of the proposed blockchain architecture are presented in Fig. 4.

Educational organizations can be either large educational institutes or some trusted party that runs the chain for the self-employed teachers and small institutions. This private chain is maintained by each educational organizations or independently of others. This private chain contains personalized information on the interactions between the students and the educational organizations. All the interactions, such as receiving an assignment, submitting solutions, or being graded, are treated as transactions in the private chain. Students get access to the platform through a Web browser and mobile applications. Using the applications, they choose educational organizations, enrol in courses, get assignments and submit solutions. The scores and the criteria of whether the student has finished the course successfully are determined by the educational organizations.

Making the educational organization' chains private opens the possibility for Educators to tamper with the data in their chains. To overcome this issue and make the private transactions publicly verifiable, it introduces a public chain. The public chain consists of Witnesses. They do so by writing the authentication information of a private block into the public chain, which is used in the future by an arbitrary

Verifier to substantiate a proof of transaction inclusion given to it by a Student or an educational organization.

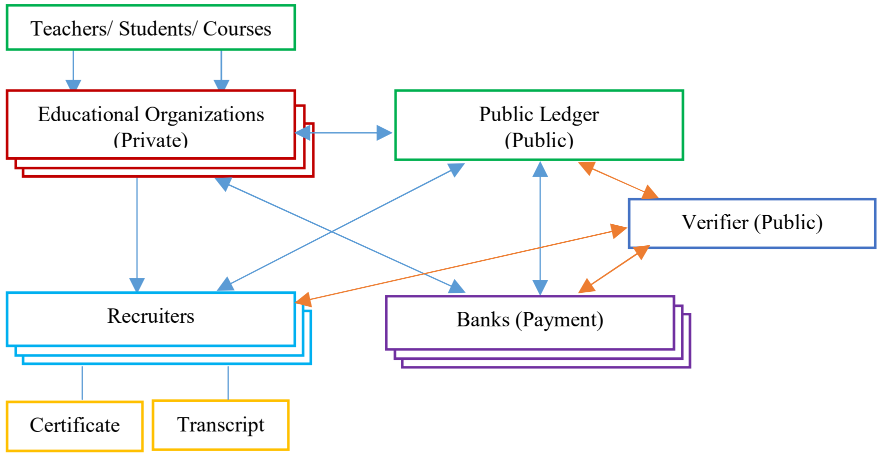

Fig 4. Proposed PETS architectural model.

The Recruiters are the entities interested in gathering data about students from educational institutions. They buy this data from the educational organization using a secure data disclosure protocol. Witnesses also ensure validity and security of every data trade, because corresponding transactions and actions of each party are also stored in public blockchain.

The entries in "blockchain" can significantly reduce the workload of both students who would end the inconvenience of making paper copies of certificates or procedures to request a course in educational institutions and they can instantly verify individual or organizational credentials.

4.8 Blockchain Architecture

The proposed blockchain architecture for higher education institutions is shown in Fig. 5.This architecture included various components and they are *data consumer, data provider, data portal, blockchain platform, data storage, a data engine***,** *blockchain access, etc*.

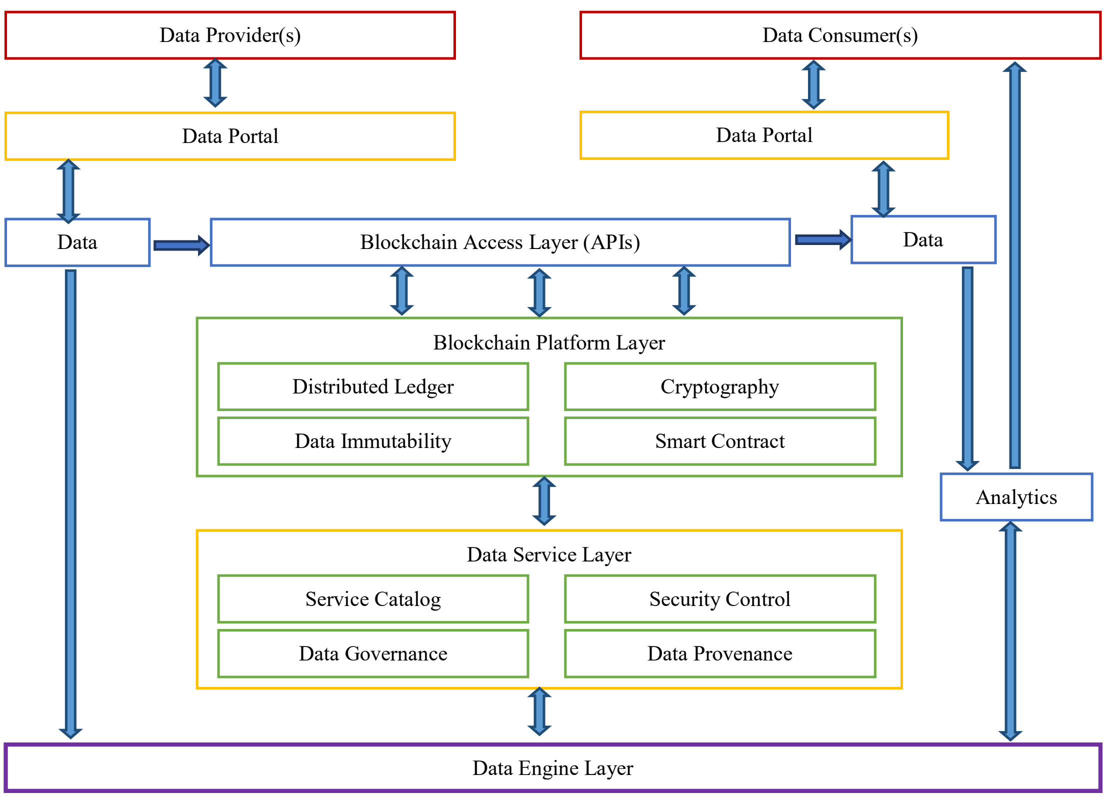

Fig 5. Proposed PETS architecture.

The key components of a proposed PETS model are as follows –

- A *data consumer* is a user interface, system or tool that uses data. Users who use data for a specific purpose and can be affected by its quality.
- A *data provider* is a user interface, system or device that collects data that is relevant to an organization.
- *Data portal* – This is the data portal that the data providers and the data consumers will use to either put up data for sale or checkout data for purchase. Given that the user experience is going to be the most critical thing for this portal to succeed, this can be assumed a custom website or a third-party portal customized with the right set of security and access built into it.
- *Blockchain platform* – It is an appropriate platform that supports some of the key capabilities – distributed ledger, support for cryptography, immutability assurance, smart contracts, oracles etc. Based on the ecosystem, the players within that and the sensitivity of the data, you may end up choosing a permissioned or permission less blockchain.
- *Data storage* – A high volume of information is being exchanged here, it needs to consider storage in terms volume, variety, the location of data and maybe sensitivity. It stores all of the actual data on-chain or off-chain. Big data storage options should be leveraged to handle such massive volumes. The "variety" factor can also determine which storage option may be structured or unstructured data.
- *Data Engine* – In order to function effectively, the connecting between the on-chain data and the off-chain data will be a set of services that offer unified security, governance, management and visibility across all data sets. This brings forth a seamless and unified data plane that both data providers and consumers can leverage easily. The services will include a data catalogue that can make data discoverability and search ability a breeze across multiple data sources.
- *Blockchain access*– There are multiple protocols or mechanisms through which a blockchain platform can be accessed. Standardizing on a common access layer that leverages something as common as *application programming interfaces* (APIs) makes it easy for the developer community around this initiative to work together easily. APIs allow for abstraction that enables a fair amount of future proofing.

The proposed architecture covered all of the above components. The proposed architecture may be required some ideal technologies for data ingestion and advanced analytics. The *data logistics platform* automates the movement of data between disparate systems. It provides real-time control that makes it easy to manage the movement of data between any source and any destination. This is perfect for the proposed architecture where different providers have different types of data to offer.

4.9 Contribution to Education Sector

The proposed architecture is ideal for a smart education powered by Blockchain. It may start changing as Blockchain itself evolves as a technology. The data privacy and compliance regulations will largely dictate the adoption or inhibition of such a model.To understand how blockchain can contribute to the education sector [11], let us have a look at Fig.6.

A student/candidate uploads degree certificates and work experience letters from past employers on a server.The educational institutions and previous employers could verify the documents. These verified documents get stored on the interplanetary file system (IPFS). It is a versioned file system, which stores files and tracks versions over time. After the documents are stored on IPFS, the IPFS then returns the document hash. The hash values of these documents can be stored into blockchain by using smart contracts. When a recruiter accesses the documents verified by past employers and educational institutions, the recruiter is assured about their authenticity. Such blockchain based verification platforms would require that the hiring employers pay a fee to get the verified candidate details.

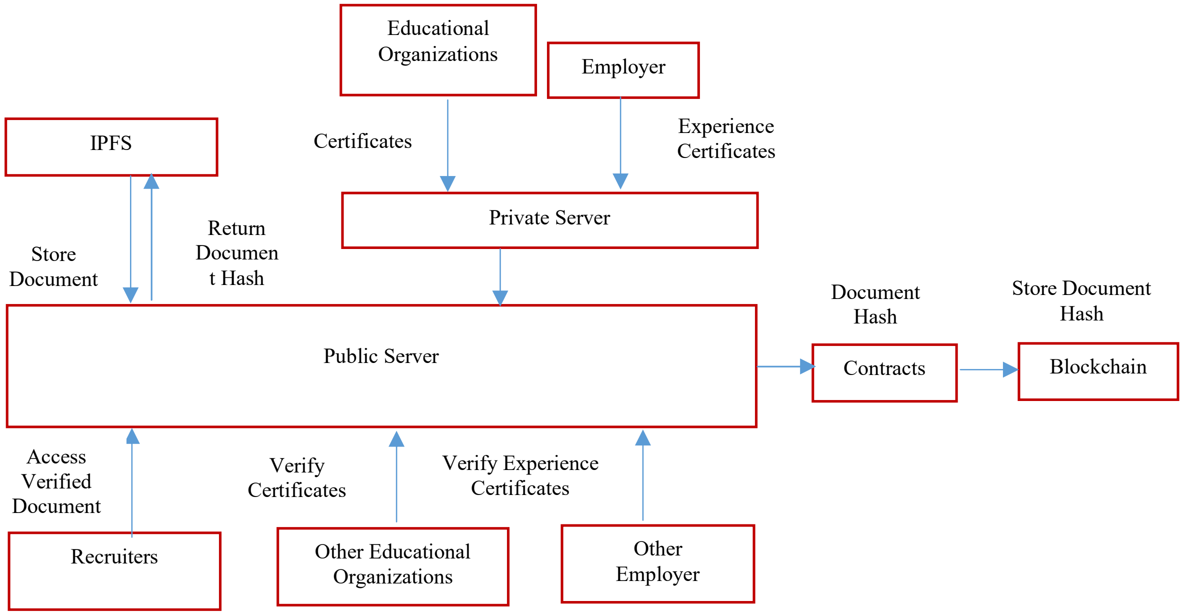

Fig 6. Deployment view in the education sector.

The blockchain-based educational applications can provide students with the ability to gain greater control over their individual education by offering flexible access to content and courses suggested based on previous successes or failures and attainment.

4.10 Results

The proposed blockchain architecture provides a rich, secure, and transparent platform on which to create a global network for higher educational learning. The blockchain architecture applies to recapture the real-time records of learning. It believes that higher education works best when it works for all types of teaching and learning. In addition, it transforms the architecture of higher education for the future generation of lifelong learners.

Education is a multifaceted sector where different systems need to adapt to prepare students for the jobs of tomorrow. Having a foolproof system that records a student's academic history before and during a working life can not only help in battling dishonesty but can also help to tackle the issues of bespoke learning. The PETS architecture can allow workers to build up a secure, verifiable digital record of formal qualifications, experience and soft skills gained over their lifetime.

4.11 Benefits and Drawbacks

There are some benefits to applying blockchain technology in education. They *increased transparency*, *accountability through smart contracts* and *incentivization of learning*.

- *Increased transparency:* Blockchains technology creates a chronological list of events that have transpired in real-time education. This is useful for verifying transcripts, showing a complete report card and keeping the students honest about their progress. Having a student submit their home via blockchain ensures that they cannot "lose" their homework or claim the teacher lost it.
- *Accountability through smart contracts:* Teachers, educational institutions administrators and students will soon be able to engage in smart contracts. For example, students and teachers could enter into a digital agreement that stipulates an assignment's parameters, due date and grading deadline. Smart contracts can also be deployed for student loan payments.
- *Incentivization of learning:*Tokenization has become a mainstay of the blockchain. Before long, academic institutions will be able to incentivize students to pay student loans on time and teachers to motivate students by awarding cryptocurrency to those who perform highly or complete a certain major. The gamification aspect of education created by tokenization has been tremendously beneficial.

It is undeniable that there are potential drawbacks of applying blockchain technology [16] in education.

- As a complex system, some learning behaviours and learning outcomes need to be reviewed by the instructors subjectively such as essays and classroom presentations. It is quite hard to evaluate this kind of learning activities by the pre-programmed smart contract without human intervention.

- If an educational blockchain system were put into use in schools, all students' educational, data would be integrated into blockchain ledgers. The immutability feature of blockchain technology would act as a double-edged sword. It removes the possibility of modifying educational record for legitimate reasons for some students.
- The classic Proof of Work consensus model wastes energy and has a poor performance in terms of a number of transactions per second, which would cost an extra expense, and hinder its application in schools.

4.12 Use Cases

Donald Clark, 2016 reported that blockchain could be implemented within individual educational institutions, groups of educational institutions, and both national and international educational bodies. In fact, anyone wanting to securely store badges, credits, and qualifications could consider using blockchain technology. Some of the use cases or examples of how blockchain is being implemented in education [24] are Blockcerts, APPII, Gilgamesh Platform, ODEM, Sony Global Education, Blockchain Education Network, Disciplina, Parchment, and BitDegree.

V. CONCLUSION AND FUTURE ENHANCEMENTS

The blockchain is essentially a distributed ledger technology, which uses the cryptography techniques and distributed consensus algorithms to create the features of decentralization, traceability, immutability, and currency properties. Blockchain has shown its potential in industry and academia. Its currency properties have the potential to trigger many innovative applications for education. It can store a complete, trustworthy set of record of educational activities including the processes and results informal as well as informal learning environments.

As proof of concept, it is proposed to design a blockchain architecture to learning solutions. This proposed PETs architecture is a global blockchain-based architecture for a higher education learning system. The proposed architecture addresses a globally unified viewpoint for learners and educational organizations. The beneficiaries of the proposed architecture are potential employers, who can directly validate the information provided by students, the learners benefit from a single and transparent view of their completed courses and the HEIs have access to up-to-date data regardless of a student's educational origins. The proposed solution is based on the distributed P2P network system.

As for data management, blockchain could be used to store important data, as it is distributed and secure. Blockchain could also ensure the data is original. When it comes to data analytics, transactions on blockchain could be used for big data analytics. Its future, it is planned to introduce the architecture based on big data analytics and an appropriate version of the blockchain technology.

REFERENCES

[1]. Alexander Grech, Anthony F, Camilleri, Blockchain in Education, Joint Research Centre (JRC), the European Commission's science and knowledge service, 2017.
[2]. Alok Kumar Jain, Blockchain Goes to School, Digital Solutions, Innovation & Domain Consulting, Cognizant's Education Practice, Cognizant 20-20 Insights, 2018.
[3]. Anirudh Bhardwaj, Using Blockchain Can Do Wonders In Education Sector. https://www.oodlestechnologies.com/blogs/Using-Blockchain-Can-Do-Wonders-In-Education-Sector, 2018,
[4]. Arati Baliga, Corporate CTO Office Understanding Blockchain Consensus Models, Persistent Systems Ltd, April 2017.
[5]. Arodek, https://arodek.com/block-chain/
[6]. Audrey Watters, The Blockchain for Education: An Introduction, http://hackeducation.com/2016/04/07/blockchain-education-guide, 2016.
[7]. BitRice, Create the optimum data storage and content sharing eco-chain, White Paper of Bit Rice (BTR), BitRice Foundation Singapore, 2018,
[8]. Blockchain News, 2018, How will blockchain technology affect higher education in the future?
[9]. Blog, Introduction to Blockchain Technology, https://netsend.com/blog/introduction-to-blockchain-technology/, 2017.
[10]. Bulletin, https://builtin.com/blockchain/blockchain-in-education
[11]. Chaitali Acharya, How can Blockchain help in Background Check?Harbinger Systems2018.
[12]. Donald Clark, 10 ways Blockchain could be used in education, https://oeb.global/oeb-insights/10-ways-blockchain-could-be-used-in-education/, 2016.
[13]. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, Blockchain Technology Overview, National Institute of Standards and Technology, Internal Report 8202, 2018.
[14]. Education, https://education.siliconindiamagazine.com/viewpoint/blockchain-is-it-the-future-to-education-nwid-8576.html
[15]. Everis, https://www.everis.com/belgium/en/page/blockchain-labour-market, 2018,
[16]. Guang Chen, Bing Xu, Manli Lu and Nian-Shing Chen, Exploring blockchain technology and its potential applications for education, Smart Learning Environments, 2018. 5:1
[17]. Ioannis Karamitsos, Maria Papadaki, Nedaa Baker Al Barghuthi, Design of the Blockchain Smart Contract: A Use Case for Real Estate, Journal of Information Security, 2018, 9, 177-190
[18]. Karamitsos, I., Papadaki, M. and Al Barghuthi, N.B., Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of In-formation Security, 9, 177-190, 2018.
[19]. Karim Sultan, Umar Ruhi and Rubina Lakhani, Conceptualizing Blockchains: Characteristics & Applications, 11th IADIS International Conference Information Systems, 2018.
[20]. Leonardo Maria De Rossi, Gianluca Salviotti, Nico Abbatemarco, Towards a Comprehensive Blockchain Architecture Continuum, Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.
[21]. Muhamed Turkanović , Marko Hölbl , Kristjan Košič, Marjan Heričko, and Aida Kamišalić, EduCTX: A Blockchain-Based Higher Education Credit Platform, IEEE Access, 2018.
[22]. Open Access, https://www.openaccessgovernment.org/how-blockchain-technology-affects-higher-education/54512/
[23]. Rachael Hartley, What is the role of blockchain in education? Cognizant Education Technology, 2018.

[24]. Sam Daley, blockchain education companies earning straight A's, https://builtin.com/blockchain/blockchain-in-education, 2018.

[25]. St. Laurent, Andrew M. (2008). Understanding Open Source and Free Software Licensing. O'Reilly Media. pp. 4.

[26]. Stefan K. Johansen, A comprehensive literature review on the Blockchain as a technological enabler for innovation, Dept. of Information Systems, Mannheim University, 2018.

[27]. Stefan Seebacher, Ronny Schüritz, Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review, Springer International Publishing AG 2017. 12–23, 2017.

[28]. Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba, A Taxonomy of Blockchain-Based Systems for Architecture Design, IEEE International Conference on Software Architecture (ICSA), Gothenburg, 243-252, 2017.

[29]. Zhaoyang Dong, Fengji Luo, Gaoqi Liang, Blockchain: a secure, decentralized, trusted cyberinfrastructure solution for future energy systems, Journal of Mod. Power Syst. Clean Energy 6(5):958–967, 2018.