BLOCKCHAIN IN VERIFICATION

SYNOPSIS:

* Introduction
* Block chain
* Characteristics of block chain
* BcER^2
* Components of BcER^2
* Implementation
* Related workings
* Working of distributed blockchain
* Conclusion

INTRODUCTION:

Blockchain is a technology considered by many to be something as relevant as the rise of theInternet. There have been experiments with blockchains since the early 1990’s, but it was onlyin 2008, with the release of a white paper by an individual or group of individuals under the pseudonym of Satoshi Nakamoto, that blockchains gained wide adoption.

BLOCKCHAIN:

Educational records are used worldwide and, from the user point of view, is an important asset for individuals pledging for scholarships, jobs and professional and academic visibility in general. Currently, our educational records management systems are mostly physically localized, require speciﬁc and non-trivial procedures to access information, are in many cases

unreliable and, ﬁnally, do not follow or have any educational standards.

CHARACTERISTICS OF BLOCKCHAIN:

Blockchain has a set of key characteristics:

consensus, provenance, immutability and ﬁnality.All relevant participants make decisions by consensus, in this process most participants must agree that a transaction is valid. This goal is achieved through the implementation of consensus

algorithms. Each network enforces the conditions under which transactions are performed or the

exchange of assets may occur. Provenance guarantees that participants know where the asset

came from and how its ownership has changed over time. With immutability, no participant can

tamper with a transaction after it has been recorded to the ledger. If a transaction is in error,a new transaction must be used to reverse the error, and both transactions are then visible.With ﬁnality, a single shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

BcER^2:

An “education record” in the context of this paper is a record containing ﬁles, documents, and

other materials which: i) Contains information directly related to the academic historical

of a student or a professional; and ii) From a local perspective are typically maintained by an

educational institution or by other entity acting for such institution.

There are signiﬁcant advantages and beneﬁts in using a Blockchain-based educational repos-

itory: i) Educational records (e-diplomas, e-certiﬁcates, other) uploaded and managed

on the Blockchain ledger are more secure and resistant to “physical wear and tear” than paper

documents; ii) Educational records are seamless and eﬃciently transferred and shared among

parties (universities, schools and employers) fostering worldwide visibility; and iii) Educational

records stored on the blockchain can be accessed any time, from any location.

In summary, educational records managed by Blockchain technology stimulate the knowl-

edge/reward principle, makes credentials more trustworthy and keeps educational records safe

and easy to access.

COMPONENTS OF BcER^2:

he basic components belonging to the the BcER2educational records repository are illus-

trated in Figure 2and basically reﬂect the business network adopted which is suitable for an

educational records repository that registers, manages and provide access to them.The ”asset information” component contains information related to the educational record being managed by BcER2. This component is responsible for asset’s deﬁnition and consistency.

The ”Business Model Information” component contains information related to the process

involved in the asset management. It deﬁnes basically the participants, name space and trans-

actions involved in the process.

The ”Transaction Process Function” component contains the information concerning the

specif functions invoke in the business model to manage the asset.

The ”Access Rules” component contains, as the name suggests, the access rules including

all priorities among participants involved in the business model adopted.

IMPLEMENTATION:

The Hyperledger Composer was used to implement the BcER2educational repository. Hy-

perledger Composer is an open source development tool set and framework aiming to support

the development of blockchain applications. It allows the modeling of the business network and

integrates existing systems components and data deploying as such the blockchain application.

The use case adopted by the actual implementation is initially intended to verify the authen-

ticity of student’s certiﬁcates generated by Salvador University (UNIFACS) under-graduation

courses. BcER2is composed of assets, participants and transactions, with each of these entities being

represented within Hyperledger framework as conﬁguration ﬁles.

The .CTO hyperledger component is responsible for implementing the assets, participants,

and transactions, including all relevant information. A Hyperledger Composer CTO ﬁle is

composed of the following elements: i) A name-space with resources declaration; ii) Resources

deﬁnition including assets, transactions, participants and events; and iii) Optional resource

import declarations from other name-spaces.The data that need to be included in each transcation block is that date of transcation,verification of that transcation ,destination of the transcation and if any new transcation had been done.The ACL hyperledger component provides declarative access control for the elements in the

domain model. By deﬁning access and control (ACL) rules you can determine which users/roles

are permitted to create, read, update or delete elements in a business network’s domain model.

The ’Business Network’ deﬁnition, from the Hyperledger Composer perspective, is composed

by a set of model ﬁles deﬁning assets, participants and transactions. The ”.JS” script ﬁle is

responsible for maintain a set of scripts. The scripts contain transaction process functions that

implement the transactions deﬁned in the ’Business Model’. Transaction processing functions are automatically invoked at run-time when transactions are submitted and their structure are composed by a JavaScript function.

RELATED WORKINGS:

In recent years, blockchain technology has been widely used as the basic construct for crypto-

coins such as Bitcoin.

MIT has a system for building Blockchain-based applications that issues and veriﬁes oﬃcial

records called ”Blockcerts Wallet”. It allows, for instance, the creation of a certiﬁcate wallet

for students to receive virtual diplomas via their smart devices. Diﬀerent from Blockchain-

based Educational Records Repository (BcER2), MIT Blockcerts Wallet system is a building

application platform that has a similar target in terms of allowing educational records creation

and dissemination using Blockchain.

New promisingly Blockchain-based solutions include ’intelligent contracts’. Ethereum, dis-

cussed in, allows the creation of contracts that are self-managed. Contracts are triggered

by an event such as passing an expiration date or achieving a speciﬁc price goal. In response,

the smart contract manages itself by making adjustments as needed and without the input of

external entities.The item that changes the ownership is that the educational institutioins authorisation towards that certificate given to him.

WORKING OF DISTRIBUTED BLOCKCHAIN:

A distributed ledger can be described as a ledger of any transactions or contracts maintained in decentralized form across different locations and people, eliminating the need for a central authority to keep a check against manipulation. In this manner, a central authority is not needed to authorize or validate any transactions.

All the information on the ledger is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures. Once the information is stored, it becomes an immutable database, which the rules of the network govern. Distributed ledgers also reduce operational inefficiencies, speed up the amount of time a transaction takes to complete, are automated, and therefore function 24/7, all of which reduce overall costs for the entities that use them. Distributed ledger technology has great potential to revolutionize the way governments, institutions, and corporations work. It can help governments in tax collection, issuance of passports, recording land registries, licenses, and the outlay of Social Security benefits, as well as voting procedures. The educational institution needs to be involved in validating degrees and transcripts. The validation system in distributed system work as such that each of the nodes or block is to be verified by all the users in that chain. The each ledger is to be verified by all the users in that network. Until all the users in the network validate the block it is considered as invalidate. Even though one user said it as invalidate it is considered as invalidate and it cannot be used further for updation of ledger. In this case if we apply for a new job and employer of the company wants to check it he can do this by checking each block with their respective institution or schools or private education providers by checking their digital signatures present in the certificate.

Conclusion:

In this work, we proposed a solution to the current challenge of connecting learning records across different institutions. One of the main contributions of this work is providing a concrete implementation of a blockchain platform that enable these features. This paper also presents an overview of the resource requirements for running such a system, and the potential benefits when compared to other alternative tools. We also discussed potential challenges and possible approaches to guide future work. While we acknowledge that the time taken to write learning records to the blockchain currently is not suitable for real-time access-based systems, we recommend its usage in scenarios where transition from one institution to another occurs over a given period of time that is within the waiting time as earlier presented. We also discussed about defining and enforcing existing user data privacy policies on the learning logs using smart contracts. While our implementation considers top-level approach of representing these permissions, it will be necessary to understand the implications of having action verb-based privacy definitions.

In future work, greater focus on detailed components of learning logs and corresponding privacy measures is required to develop standardized formats for representing permissions on the blockchain. The scalability of the current BOLL system should also be investigated to ensure that it can handle being implemented as a wide-reaching system.