**MORALITY CERTIFY AGAINST ARBITER AUDITOR USING BLOCKCHAIN**

**MORALITY CERTIFY AGAINST ARBITER AUDITOR USING BLOCKCHAIN**

**Preface**

**TABLE OF CONTENTS**

1. SOFTWARE DEVELOPMENT LIFE CYCLE

2. PLATFORM KNOWLEDGE

3. DOMAIN KNOWLEDGE

4. ABOUT THE PROJECT

4.1 ABSTRACT

4.2 SCOPE OF THE PROJECT

4.3 EXISTING SYSTEM

4.3.1 DISADVANTAGES

4.4 PROPOSED SYSTEM

4.4.1 ADVANTAGES

5. BOTTOM LINE AND FUTURE ENHANCEMENT

6. HARDWARE AND SOFTWARE REQUIREMENTS

**1. SDLC (Software Development Life Cycle)**

The Software Development Life Cycle is a systematic process for building software that ensures the quality and correctness of the software built. SDLC process aims to produce high-quality software which meets customer expectations. The software development should be completed within the pre-defined time frame and cost.

**SDLC Phases**

The entire SDLC process is divided into the following stages:



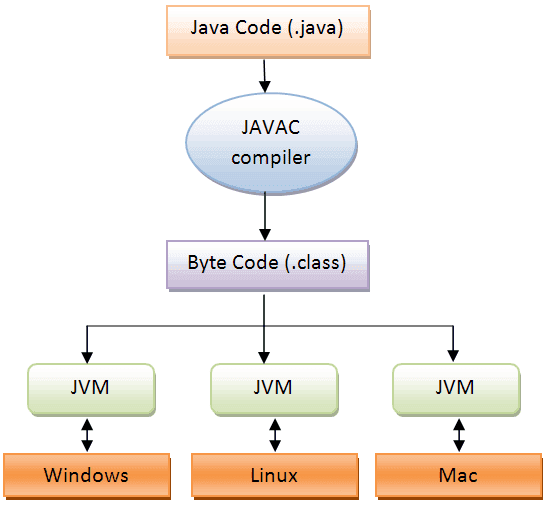
* Phase 1: Requirement collection and analysis
* Phase 2: Feasibility study
* Phase 3: Design
* Phase 4: Coding
* Phase 5: Testing
* Phase 6: Installation/Deployment
* Phase 7: Maintenance

**2. Platform Knowledge**

**Introduction to java**

Java programming language was originally developed by Sun Microsystems which was initiated by James Gosling and released in 1995 as a core component of Sun Microsystems' Java platform.Initially, the language was called “Oak” but it was renamed as “Java” in 1995.The primary motivation of this language was the need for a platform-independent language. Finally, Java is for Internet Programming where C was to System Programming.

**Java architecture**

Java is a high-levelObject-oriented programming language. A program written in high level language cannot be run on any machine directly. First, it needs to be translated into that particular machine language. The javac compiler does this thing, it takes java program (.java file containing source code) and translates it into machine code (referred as byte code or .class file). Java Virtual Machine (JVM) is a virtual machine that resides in the real machine (your computer) and the machine language for JVM is byte code. JVM executes the byte code generated by compiler and produce output. JVM is the one that makes java platform independent.

**3.DOMAIN KNOWLEDGE:**

**BLOCK CHAIN**

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed time stamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a *value-exchange protocol*. This blockchain-based exchange of value can be completed quicker, safer and cheaper than with traditional systems. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

**Block Chain Analytics:**

Blockchain analysis is the process of inspecting, identifying, clustering, modeling and visually representing data on a cryptographic distributed-ledger known as a blockchain. Data in most blockchains are public meaning that anyone can harness the addresses. By using common-spend clustering algorithms, it is possible to map the spending of certain entities on the blockchain. This is how criminals have been caught moving illicit funds using various crypto currencies The goal of blockchain analysis is discovering useful information about the different actors transacting in crypto currency. Analysis of public blockchains such as the bitcoin and ethereum is often conducted by private companies Bitcoin has long been associated with the trade of illegal goods on the dark web; this has been the case since bitcoin became the standard currency on the now closed Silk Road. Crypto currency exchanges are increasingly required by law to address the source of funds for crypto traders. Singapore, Japan, the USA are examples of countries that have passed laws that now require the exchanges to track the source of the crypto funds.

**MORALITY CERTIFY AGAINST ARBITER AUDITOR USING BLOCKCHAIN**

**4. About the Project**

**4.1 Abstract**

The sending of distributed storage administrations has critical advantages in overseeing information for clients. Be that as it may, it likewise causes numerous security concerns, and one of them is information uprightness. Open check methods can empower a client to utilize an outsider evaluator to confirm the information honesty for the benefit of the organization, while existing open confirmation plans are defenseless examiners who may not perform confirmations on schedule. In this paper we propose a third-party auditor delegated for the background verification process which is done on the part of every organization. In our project a novel way of verification introduced which implements the block chain technology. With the use of blockchain technology, the candidate's identity and the data about him or her stocked in the database will be completely protected from any unauthorized access. We use this technology to access the related previous data about a candidate who is going to be verified by the auditor, by providing a unique identity for the each entity involved in the verification process. A blockchain is essentially a digital ledger of data that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of data, and every time a new data occurs on the blockchain, a record of that data is added to every participant’s ledger. That while it is called decentralized database management. After the processgets over, the auditor will update the results status into the database and then the candidate will be available to the organization for further process. By the usage of this block chain technology the background details of the persons will stored in a confidential manner.

**4.2 Scope of the project**

Our proposal is to design a verification scheme that will resist the activities of malicious parties. There is a key idea behind this system, which is to utilize Blockchain technology, which provides a tamper-proof and distributed way for verification to be conducted without the need for a central authority or a trusting third party. A data user may be a company or a person with some of the most valuable data available, depending on who the data belongs to. The data must be accumulated by a central storage and those data verified with some of the third-party auditors for data integrity. The main scope of the project is to verify the candidate data by the auditing entity. By using the block chain technology, the verification of auditors and the data integrity which is stored in the database, were achieved. Thus, it reduces the trust related problem associated with the auditors involved in the verification.

**4.3 Existing System**

Existing public verification schemes require the auditor to perform the verification periodically by direct contact so that the data corruption can be detected as soon as possible. It cannot resist an auditing activity that perform the data integrity verification on schedule and deviate from the original objective of verification schemes**.**  Actually, periodical verification can reflect the state of integrity of the outsourced data in each period, which enables the auditor to find the data modified by direct contact. Any time the malicious data outsourced by the provider, the auditing entity can find it within the period, stops to use the corrupted record. And the centralized unique Id is not maintained for the entity so that the verification is somewhat difficult. And there are no such methodologies to verify the details in an automated way.

**4.3.1 Disadvantages**

* Data integrity is difficult to manage and maintain in the existing system.
* An auditor who is working on behalf of a third party may be capable of performing malicious activities.
* Management problem existing in most of the existing public verification schemes.
* The existing schemes cannot resist an entity that performs malicious activities for the process.
* During the accessing of data, it is questionable as to what level of security that data is in.

**4.4 Proposed System**

The proposed system overcomes the problem of existing scheme by providing a verification scheme which is performed by the auditor. It consists of two phases, in the first phase, the auditor verifies the integrity of outsourced data which is the data provided by the data provider/user. The outsourced data is in the second phase, the auditor utilizes the connected data in the block chain and the verification is done by retrieving the information and perform matching operation between the data where each verification performed by the auditor only, and it is integrated by the block chain.The key idea is to require auditors to record each verification result into a database. The original data of the entity will be stored in the organization once is it verified. And retrieval of the chain is based on the key identification from the information provided by the candidate.

**4.4.1 Advantages**

* + - It is through the use of auditors that malicious activities are restricted.
    - A unique ID is used to store and maintain the data of users so that it can be located by the use of Blockchain.
    - Verification overhead on many data will be minimized.
    - Management of the data integrity will be optimized.
    - User’s privacy data will be protected even if there is a misleading entity.

**5. Bottom line and Future Enhancement**

In this paper we proposed a verification scheme on the outsourced data of the candidate by the recognized auditor delegated by the organization. It utilizes the chain properties, where each verification performed by the auditor is integrated into the Block chain. The analysis demonstrates that it provides the security guarantee with existing schemes of data verification. In the comprehensive performance analysis, which demonstrates that the it has constant communication overhead and is efficient in terms of computation overhead? We will also investigate how to utilize Block chain technology to enhance the auditing system in terms of security, performance, and functionality. As the outsourced data processing has also played an important role in current information age, we will explore the integration of Block chain into existing schemes which should have a deep impact on outsourced data processing.

**6. HARDWARE AND SOFTWARE REQUIREMENTS**

**Hardware requirements:**

* Processor : Intel (R) Pentium (R)
* Speed : 1.6 GHz and Above
* RAM : 4 GB and Above
* Hard Disk : 120 GB
* Monitor : 15’’ LED SVGA
* Input Devices : Keyboard, Mouse

**Software requirements:**

* Operating system : Windows 7 / 8 / 8.1 / 10
* Coding Language : JAVA / J2EE
* Java Version : JDK v8
* IDE : Eclipse Oxygen / Neon
* Database : MySQL v5.1
* Database Tool : HeidiSQL v11.0
* Application Server : Apache Tomcat 8.x / 9.x