BMS INSTITUTE OF TECHNOLOGY & MANAGEMENT

YELAHANKA, BENGALURU - 560064.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VTU Mini Project – 6th Semester CSE

2019-20 Even Semester

Synopsis of Computer Graphics & Visualization Laboratory 17CSL68
Mini Project work

"BLOCKCHAIN SIMULATION"

Submitted By

ARUN SHENOY USN: 1BY17CS032

CHARAN KALSHETTY USN: 1BY17CS041

Under the guidance of

Mr. Shankar R
Assistant Professor
CSE, BMSIT&M

2019-2020

Abstract

A block-chain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

By design, a block chain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a block chain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although block chain records are not unalterable, block chains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a block chain.

Introduction

A block-chain is a decentralized, distributed, and oftentimes 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 block-chain 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 block-chain 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 block-chain has been described as a value-exchange protocol. A block-chain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blocks:

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the block-chain, linking the

two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

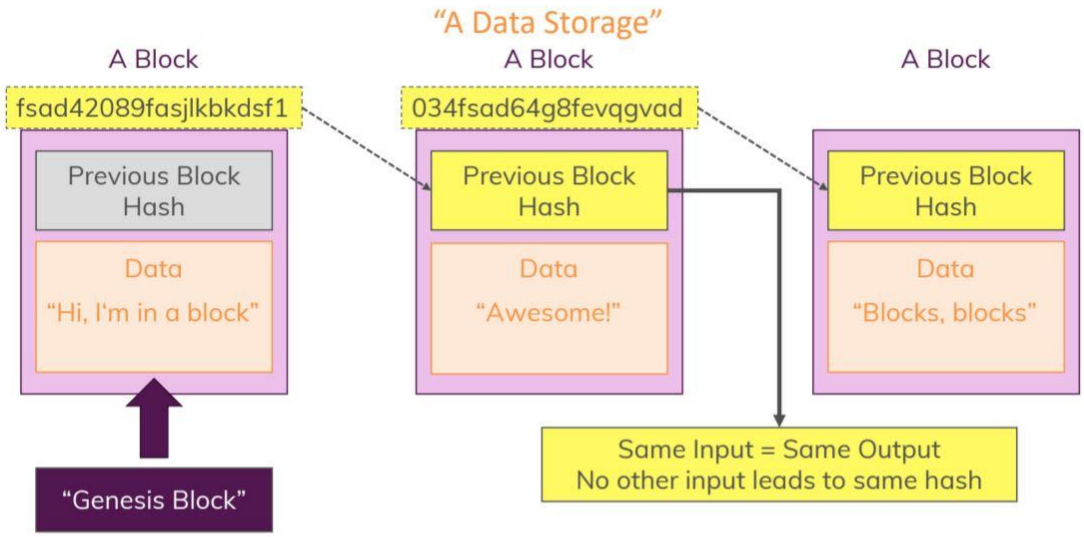

Fig: Simple Block-chain

Decentralization:

Peer-to-peer block-chain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Block-chain security methods include the use of public-key cryptography. A public key (a long, random-looking string of numbers) is an address on the block-chain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that block-chains now support. Data stored on the block-chain is generally considered incorruptible.

Motivation

Since block-chain is a new and emerging technology it is hard for people, sometimes even computer scientists to understand the exact working of the block-chain and the best way to understand something is to visualize it. We hope to make use of the concepts learned in

computer graphics to help people visualize and clearly understand the working of a block-chain. This includes how blocks are mined, how transaction data is stored in blocks and how these blocks themselves are linked to each other to form a block-chain.

Existing System

There are many websites and videos to help people understand the concept and visualize the processes in block-chain. “blockchain.com” is one such website. Many YouTube videos are also available to understand the same.

Limitations of Existing System

The existing system for visualizing a block-chain does not keep in mind about the people who are new to this technology. It assumes that the viewers are well versed in block-chain jargon and hence is very technical and many people find it difficult to follow the concept. It is noticed that most the existing systems are not interactive with the user.

Proposed System

Our simulation keeps in mind viewers and users who are not familiar with the block-chain technology and starts from the very basic of what a block is to how blocks are linked to each other. It also deals with how nodes store block-chain and communicate with each other.

System Requirement Specifications

Functional Requirements:

1. Users should be able to understand the basic concepts involved in block-chain.
2. Users should be able to interact with the system to gain even better understanding.

Non Functional Requirements:

1. Simple to use and understand.
2. Done on OpenGL hence very light-weight.

Proposed Methodology

The idea is to help all the viewers get a basic idea of how a block chain works. We use simple OpenGL methods in C++ to create a visualization of the block and the chain. These help the user to get an idea of what a block means and how the blocks are linked to each other giving rise to the term block-chain.
The simulation also explains what takes place when a sender A sends a certain amount to recipient B. This includes how a transaction is placed in open transactions and the mined into a block.

References

1. https://en.wikipedia.org/wiki/Blockchain - Wikipedia
2. https://www.blockchain.com/ - Block-chain website
3. Prescribed VTU CG textbook- James D Foley Computer graphics with OpenGL: pearson education