Decentralized Banking Application using Block chain Technology

Yash Amesar, Yash Nerkar, Nitesh Mali, Ashwin Nitnaware, Dr. Prashant Yawalkar.

Department of Computer Engineering, MET's Institute of Engineering, Nashik,

Maharashtra, India.

ABSTRACT

Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it's a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks. Satoshi Nakamoto described design of Bitcoin digital currency in his research paper posted to cryptography listserv in 2008. Nakamoto's suggestion has solved long pending problem of cryptographers and laid the foundation stone for digital currency.

KEYWORDS: Blockchain, Decentralized, Bank.

1. INTRODUCTION

This section describes the term Block chain and introduces the concept of Blockchain Framework. It also gives the overview of the Block chain Framework which describes the deliverables of the project.

1.1 Overview

Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it's a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks. Satoshi Nakamoto described design of Bitcoin digital currency in his research paper posted to cryptography listserv in 2008. Nakamoto's suggestion has solved long pending problem of cryptographers and laid the foundation stone for digital currency. This Chapter explains the concept, characteristics, need of Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking, financial institutions and adoption of Internet of Things (IoT). The cost of cyber-crime costs quadrupled from 2013 to 2015 however a large portion of cybercrime goes undetected. Gartner report says cost of cyber-crime is expected to reach $2 trillion by 2019 [1]. IBM's CEO, Ginni Rometty said that cybercrime is the greatest threat to every company in the world at IBM Security Summit [2]. Around two years ago Standard Chartered lost around $200 million in a fraud at China's Qingdao port [3]. Banking and financial institutions are using Blockchain based technology to reduce risk and prevent cyber fraud. For example, Nasdaq has announced its plan to launch Blockchain based digital ledger technology which will help to boost their equity management capabilities. Standard Chartered is partnering with DBS Group to develop an electronic invoice ledger using a Blockchain. The Blockchain metadata is stored in Google's LevelDB by Bitcoin Core client [5]. We can visualize Blockchain as vertical stack having blocks kept on top of each other and the bottommost block acting as foundation of the stack. The individual blocks are linked to each other and refers to previous block in the chain. The individual blocks are identified by a hash which is generated using secure hash algorithm (SHA-256) cryptographic hash algorithm on the header of the block [5]. A block will have one parent but can have multiple child each referring to the same parent block hence contains same hash in the previous block hash field. Every block contains hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as Genesis block.

2. Literature Survey

In this chapter we will see the various studies and research conducted in order to identify the current scenarios and trends in digital learning and also the attempts of introducing mobile devices in education.

2.1. Bitcoin : A peer to peer Cash System , by Satoshi Nakamoto

Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on network to edit the ledger in a secured way which is shared over distributed network of the computers. For making any changes to the existing block of data, all the nodes present

in the network run algorithms to evaluate, verify and match the transaction information with Blockchain history.

2.2. Evolution towards CYBER SECURITY by VSAE As part of the discussions at the 2013 VSAE Annual Conference (www.vsae.org), data and currency have similar challenges [6]. To protect the data, the platform approach will utilize built-in security and privacy controls within big data and data management services, including data masking, discovery, and audit. Taking the API approach, we can then combine the security API with other APIs including IoT (Internet of Things), DevOps, Cloud Integration, Mobile and Business Analytics.

2.3. Managed Blockchain by Greg Luckock Blockchain is a distributed ledger technology, commonly used in the crypto currency Bitcoin. The Financial Times (2016) defines Blockchain as a \network of computers, all of which must approve a transaction has taken place before it is recorded, in a `chain' of computer code. The details of the transfer are recorded on a public ledger that anyone on the network can see." The proposal was to distribute electronic transactions rather than maintain dependency on centralized institutions for the exchange. When looking at Bitcoin the new concept is the Blockchain framework based on research for time stamping packages and protecting the chain of custody. Blockchain is essentially a simplified payment verification system. Bitcoin and by extension, Blockchain, are realizing steady growth. At the time of this chapter, statistics from Blockhain.info indicate a 314.7M in transactions per day. Despite the growth, many questions surround widespread adoption of Bitcoin. However, the underlying framework has gained attention with application outside of the financial world.

2.4. Cloudbased Smart Health-care Platform to tackle Chronic Disease by Saman Sargolzaei, Ben Amaba, Mohamed Abdelghani"

The objective of the current work was to design and develop a cloud-based smart health data analysis platform for real-time patient-specific health monitoring and analysis with long-term surveillance to support learning based information processing system benefiting from cloud and mobile technologies. A DevOps approach to cloud-based applications development was used to create a platform for remote health data recording.

2.5. Blockchain beyond Bitcoin by S. Underwood

As an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, blockchain has attracted intensive attention in both research and applications in recent years. The key advantage of this technology lies in the fact that it enables the establishment of secured, trusted, and decentralized autonomous ecosystems for various scenarios, especially for better usage of the legacy devices, infrastructure, and resources. In this paper, we presented a systematic investigation of blockchain and cryptocurrencies. Related fundamental rationales, technical advantages, existing and potential ecosystems of Bitcoin and other cryptocurrencies are discussed, and a six-layer reference model of the blockchain framework is proposed with detailed description for each of its six layers. Potential applications of blockchain and cryptocurrencies are also addressed. Our aim here is to provide guidance and reference for future research along this promising and important.

2.6. How blockchain technology will disrupt financial services firms by B.Libert,M.Beck and J.Wind Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it's a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks.

2.7. Multi-signature addresses by M. Rosenfeld

The private keys needed to spend from a wallet can be spread across multiple machines, eliminating any one of those machines as a single point of failure, with the rationale that malware and hackers are unlikely to infect all of them. The higher the number of keys required to spend the funds (ie the higher M is in M-of-N), the more difficult it would be for an attacker to successfully steal your funds, however the more cumbersome actually using that wallet becomes. The multisig wallet can be of the m-of-n type where any m private keys out of a possible n are required to move the money. For example a 2-of-3 multisig wallet might have your private keys spread across a desktop, laptop, and smartphone, any two of which are required to move the money, but the compromise of any one key cannot result in theft. This can be used in conjunction with hardware wallets. By requiring that keys from multiple hardware wallets sign transactions, it can vastly reduce the likelihood that a malicious party that handled your hardware wallet could steal your funds, because in order for it to do that, the malicious party would have to compromise multiple hardware wallets. If each hardware wallet you use in a multisig wallet is made by a different company, it would be incredibly difficult for them to secretly conspire on an attack.

3. Problem Definition

This section explains the need of Blockchain Framework and also describes the importance of high quality Blockchain education. It introduces the basic concept of the role of Blockchain devices in learning.

3.1. Need of blockchain Technology

Digital world has produced efficiencies, new innovative products, and close customer relationships globally by the effective use of mobile, IoT (Internet of Things), social media, analytics and cloud technology to generate models for better decisions. Blockchain is recently introduced and

revolutionizing the digital world bringing a new perspective to security, resiliency and efficiency of systems. While initially popularized by Bitcoin, Blockchain is much more than a foundation for crypto currency. It offers a secure way to exchange any kind of good, service, or transaction. Industrial growth increasingly depends on trusted partnerships; but increasing regulation, cybercrime and fraud are inhibiting expansion. To address these challenges, Blockchain will enable more agile value chains, faster product innovations, closer customer relationships, and quicker integration with the IoT and cloud technology. Further Blockchain provides a lower cost of trade with a trusted contract monitored without intervention from third parties who may not add direct value. It facilitates smart contracts, engagements, and agreements with inherent, robust cyber security features. This paper is an e ort to break the ground for presenting and demonstrating the use of Blockchain technology in multiple industrial applications. A healthcare industry application, Health chain, is formalized and developed on the foundation of Blockchain using IBM Blockchain initiative. The concepts are transferable to a wide range of industries as finance, government and manufacturing where security, scalability and efficiency must meet.

3.2. Basic Concept

The cost of cyber-crime costs quadrupled from 2013 to 2015 however a large portion of cybercrime goes undetected. Gartner report says cost of cyber-crime is expected to reach $2 trillion by 2019. IBM's CEO, Ginni Rometty said that cybercrime is the greatest threat to every company in the world at IBM Securit Summit. Around two years ago Standard Chartered lost around $200 million in a fraud at China's Qingdao port. Banking and financial institutions are using Blockchain based technology to reduce risk and prevent cyber fraud. For example, Nasdaq has announced its plan to launch Blockchain based digital ledger technology which will help to boost their equity management capabilities. Standard Chartered is partnering with DBS Group to develop an electronic invoice ledger using a Blockchain. Blockchain can play crucial role in Internet of Things (IoT) and development of smart systems since we can track the history of individual devices by tracking a ledger of data exchanged. It can enable smart devices to act like an independent agent which can autonomously perform several transactions. For example, smart home appliances competing with one another for priority so that laundry machine, thermostats, dish washer and smart lighting run at an appropriate time to minimize cost of electricity against current grid prices. Another example could be smart vehicles which can diagnose any problem and schedule to pay for its maintenance.

4. Analysis

This section describes the project plan adopted and determines the requirement analysis. We have implemented the project on the basis of Rapid Application Development (RAD) model and Model View Controller (MVC) model. The stake holders who participated in the requirement analysis process were the developers of Cognifront who will be among the end users of the Blockchain Framework for building Blockchain Applications.

4.1. Requirement Analysis

4.1.1. Necessary Functions

Deliver a reusable piece of code. Build an application and

Deployment of application built onto the tablet.

4.1.2. Desirable Functions

Typical User Interface.
Transaction Manager.
Interactive System.

Fast and Convienent.

5. Design

This section describes the Software Requirement Specification (SRS) to be implemented for Maggie. It also explains the architecture of the system and external interface requirements. We have also described the Risk assessment strategy and the Data Flow Diagram which explains the flow of the project.

5.1. Project Scope

Blockchain technology is the growing invention which includes a chain of blocks. A Blockchain is a distributed or a digital ledger, which is primarily created to record the details of each financial and non-financial transaction. The absolute and permanent data is stored in a distributed database. The entire record is completely transparent which means that anyone who is linking to the network is able to view the transactions. Fundamentally, the Blockchain technology is the combination of three technologies, i.e. private key cryptography, P2P network, and the program. The Blockchain technology has shown its revolution in the field of information registration and distribution which removes the requirement for an intermediary expert to enable the digital relationships. Blockchain technology has provided the most popular product, i.e. Bitcoin which is a type of cryptocurrency and functions as a public ledger for all transactions happening on the network. It has resolved the problem of double spending, unauthorized spending, and thus increasing security. It also helps to remove the need for an intermediary expert. Since there has been a substantial increase in the number of cyber-attacks recently, the Blockchain technology help to attract the varied audience. Blockchain technology has a great future worldwide. An incredible scope of Blockchain technology has been observed in the financial field. The financial organizations were not able to sufficiently handle the heavy workload after demonetization and thus brought out the problems of having a centralized specialist for handling the financial transactions. As a result, the RBI is inspiring banks to encourage digitization. They have also released a statement which emphasized the probability of Blockchain to fight faking and the chances of bringing about particular modifications in the working of financial markets, collateral identification and payment system. Incorporating Blockchain with financial transactions gives out amazing benefits, such as a significant amount of time and money

could be saved, including a drastic reduction in time needed for processing and validating transactions. The blockchain functions on a distributed database which make the operations smoothly, ensuring tight security, and made it safe from cyber-attacks.

5.2. Software Requirement Specifications

The Software Requirement Specification describes the scope of the project, operating environment, user characteristics, design and constraints. It also elaborates the System architecture of the Blockchain Framework.

5.2.1. Operating Environment

We propose a blockchain Framework for developers to develop learning application with ease of operations that will save the time for developing the application as the reusable piece of code will be provided in our framework. Furthermore, this application can be used by the user for learning anywhere and anytime required with interactivity and portability.

5.2.2. User Classes and Characteristics

The user who is going to operate the system should have the tablet or phone having android as the base operating system.

5.2.3. Design and Implementation Constraints

Using mobile devices like phones, tablets, and laptops (with touch interface) has a very different set of challenges. The issue is not whether you have larger screen but fundamentally they are different. Battery life, screen size, form factor, variations in keyboard availability and dynamically changing orientation (horizontal or vertical positioning done by user) present using set of issues to be dealt with. The sponsoring organization Cognifront develops teaching tools software as well as self-learning aids for students. Keeping in mind vision of Cognifront, it was necessary to innovate the space where maximum number of users would benefit. Mobile devices including phones and tablets are the most prominent majority and also have high projections for the future. So it is imperative that we have to have good tools for content creation and dissemination. Teachers who are our prime focus must have some superb tools to create their blockchain. And students, who will eventually consume these modules, must have excellent tools to use these blockchain units. Out of this exact need, Maggie was born. Maggie must be extremely portable, FREE to use and open source. Our philosophy is to make world a better place.

Following are the merits of the design implementation:

Portability: As it is blockchain, on the move learning is achieved anywhere and anytime.

Delivery Mechanism: It is convenient to develop application and even very easy to use.

User-friendly: It is user-friendly due to the use of mobile devices like tablets.

5.2.4. Assumptions and Dependencies

Recent improvements in technology and computer industry such as emergence of web, online shopping and online banking consequently, has created some alternatives for traditional money exchange. As reports in first half of 2014 in [1] illustrates, number of users using online payment services and mobile banking have increased and gained a lot of popularity. However, having a centralized trusted counter party that issues and stores these transactions such as banks and services like PayPal has always been controversial. People need to trust these third parties and since they are built as a centralized system, any breach in the network can result in information loss. There has been many reports about stolen credentials and credit cards information from the banks and other services which concern people about their privacy and security.

5.3. System Architecture

The blockchain is a chain of blocks which contain specific information (database), but in a secure and genuine way that is grouped together in a network (peer-to-peer). In other words, blockchain is a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized. To make it even simpler, the blockchain concept can be compared to working on the same Google Doc simultaneously.

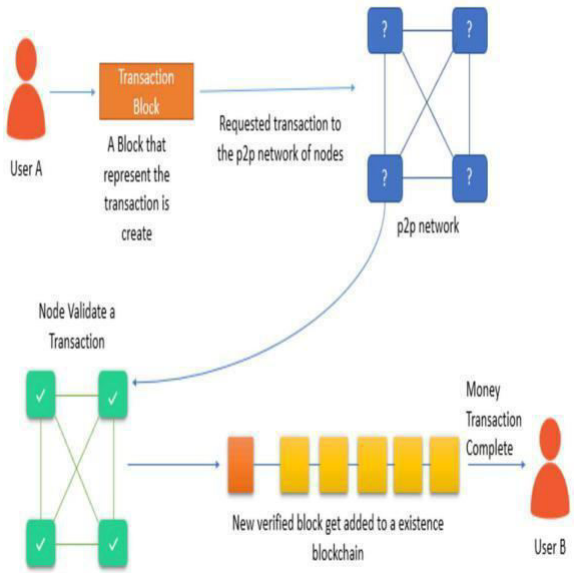


Figure 5.1: Blockchain System Architecture

Describes how Blockchain technology can improve the system efficiency while optimizing security and scalability. A sample lifecycle of an individuals' PHI where each of the networks (Urgent Care Network, Primary Care Physician (PCP), and Referral Network) create and update their own versions of PHI. In this scenario, each network may/may not have access to the full updated version of the PHI (Original updated version hypothetically kept with the patient) and therefore may not be providing the individual with proper diagnosis and treatment. The other disadvantage of the currently utilized scenario its requirement for the patient to fill out the questionnaires based on which a new copy of the PHI is created for each individual network and is kept locally. Prior explanation on the exponential growth of the use of mobile devices technologies in each of the involved networks could potentially increase security concerns due to the fragmented supporting information system. Considering individuals' PHI as a digital asset, Blockchain technology offers a robust solution where every authorized provider,

including patient, can access, analyse and update an agreed record (shared ledger) of the PHI, irrespective of the network they belong to. A proposed Blockchain implementation of the lifecycle of PHI, which we refer to it as HealthChain, targets multiple facets of the optimized design simultaneously. The patient creates the first version of the PHI record during initial visit to one of the provider networks. Initial version of the PHI (our digital asset in the chain) is then loaded on to the Blockchain. Utilization of the Smart Contracts [06], [07] insures that the patient can only create the initial version of PHI and load it onto the Blockchain.

5.4. External Interface Requirement

5.4.1. User Interfaces

Desktop Application: Using the desktop application the end user will be able to provide the blockchain content for the application to be developed using the blockchain Framework.

Blockchain Application: The blockchain application will provide a Graphical User Interface which will consist of several screens which the end user will be able to navigate to consume learning.

5.4.2. Hardware Interfaces

Mobile Devices: The blockchain applications built using the framework will be deployed on mobile devices like smart-phones and tablets supporting Android operating system version 2.2 and above.

SD card: The blockchain application will load the learning content stored on the SD card. End user will be able to write on the SD card as well.

5.4.3. Communication Interfaces

The blockchain application will be communicating through the internet via a Transmission Control Protocol of the TCP/IP suite for Social Networking Interface (SNI) and video streaming.

5.5. Software System Attribute

Reliability: The blockchain applications built using the framewok should ensure that the SD card is mounted on the device. Internet facility must be available for using the feature of Social Networking Interface and video streaming.

Availability: The blockchain application shall be available and running in a stable state at all times.

Maintainability: The blockchain framework shall be available to the developers for developing theri own blockchain applications.

Portability: The blockchain application can be used regardless of the time and location constraints.

5.6. Nonfunctional Requirement

blockchain systems represent a broad class of software systems with complex characteristics that tend to make evaluation difficult. The educational potential of mlearning contents, both as a learning and teaching tool, is widely acknowledged, and various initiatives undertaken encourage the integration of educational multimedia resources in school practice. There is a need to develop richer models for capturing and analysing NFRs in Software Engineering. However this not a simple enterprise. blockchain is so new that we are only beginning to see the potential of mobile devices in training and performance support.

Following are the Non Functional Requirements of blockchain Framework:

Small screen size of mobile devices: Mobile devices are small, portable and compact. They can often fit in a pocket or purse. Unlike laptop computers, lightweight, and some work a very long time on a charge or a couple of standard disposable or rechargeable batteries. The small screen size of mobile devices makes some people questions their worth as blockchain delivery tools. The truth is, some of these devices also have good audio capability, allowing students to listen to a narrated lecture, rather than read material on a small screen.

Input capabilities: Input capabilities of some of these devices, questioning students' ability to enter large amounts of text into a device to take notes or answer an essay-type question.

Extremely Adaptable: Many of these devices, however, are extremely adaptable and can be attached to a full-size folding keyboard that makes entering large amounts of information every bit as fast as with a conventional computer.

As mobile devices evolve and people discover new ways in which mobile devices functionalities can be applied to training, mobile blockchain will likely become something increasingly different from conventional blockchain.

5.7. Data Flow Diagram

The Data Flow Diagram of the blockchain Application developed using the blockchain Framework is as shown in Figure 5.2. The Data Flow Diagram explains the flow of information in the project that is it indicates from where information (data) is received (inputs) and where information is send (outputs).

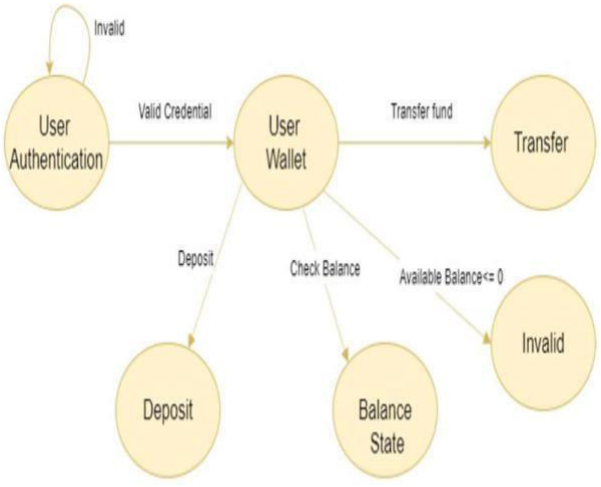


Figure 5.2: Data Flow Diagram

6. Modelling

6.1. Use Case Diagram

A use case diagram is a type of behavioral diagram defined by the UML created from a use case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals represented as use case and any dependencies between those use cases. Four modelling elements make up the use case diagram; these are:

Actors: Actors refer to a type of users, users are people who use the system. In this case student, teacher developer are the users of the framework and application Use cases: A use case defines behavioural features of a system. Each use case is named using a verb phrase that express a goal of the system. The name may appear inside or outside the ellipse.

Associations: An association is a relationship between an actor and a use case. The relationship is represented by a line between an actor and a use case. They include relationship: It is analogous to a call between objects. One use case requires some type of behaviour which is fully defined in another use case.

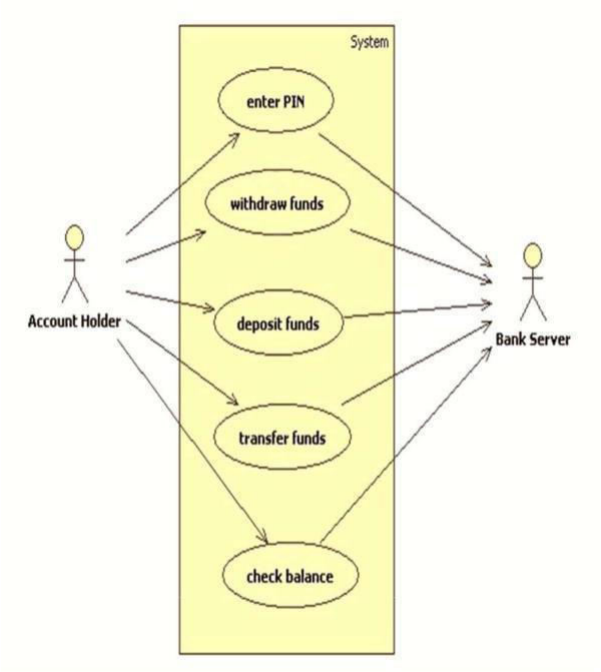


Figure 6.1: Use Case Diagram

6.2. Class Diagram

The class diagram shows the building blocks of any object oriented system. Class diagram depicts a static view of the model or part of the model, describing what attributes and behaviour it has rather that the detailing the methods of achieving operations. Class diagrams are most useful in illustrating relationships between classes and interfaces. Generalizations, aggregations, and associations are all valuable in reflecting interface, composition or usage and connections receptively. The Figure 6.2 illustrates aggregation relationships between classes. The lighter aggregation indicates that the class Object Explorer used Thumb Nail, but does not necessarily contain an instance of it. The strong, composite aggregations by the other connectors indicate ownership or containment of the source classes by the target. Class, for example Video Player values will be contained in Table of Contents

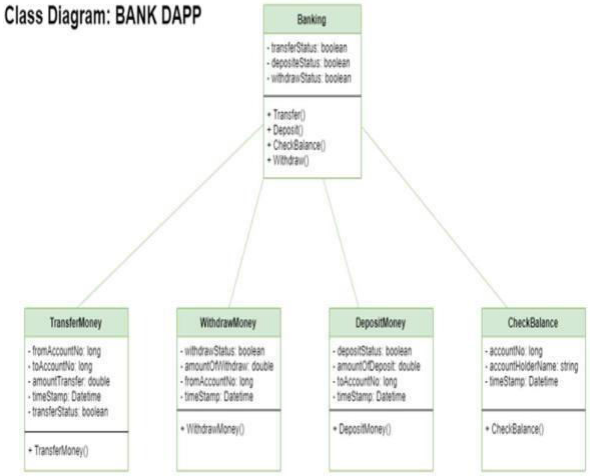


Figure 6.2: Class Diagram

6.3. Sequence Diagram

The sequence diagram is used primarily to show the interactions between objects in the sequential order that those interactions occur. Developers typically think sequence diagrams were meant exclusively for them. However, an organization's business staff can find sequence diagrams useful to communicate how the business currently works by showing how various business objects interact. Sequence diagrams illustrate how objects interact with each other. They focus on message sequences, that is, how messages are sent and received between a numbers of objects. The main purpose of sequence diagram is to show the order of events between the parts of system that are involved in particular interaction. The basic element of sequence diagram is collection of participants, that is, the parts of the system that interact with each other during the sequence. The participants are arranged horizontally with no two participants overlapping each other. in Figure 6.4 developer, framework, applications are some examples of participants. A message is communication between objects that conveys information with the expectation that action will be taken. An event is any point in an interaction where something occurs. Message can flow in whatever direction makes sense for the required interaction from left to right, right to left, or even back to the Message Caller itself.

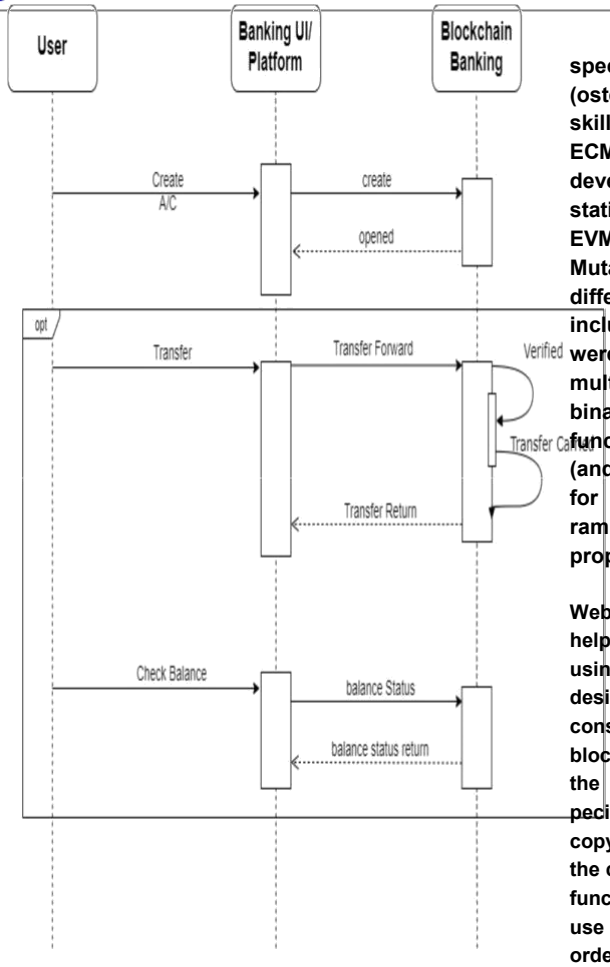


Figure 6.3: Sequence Diagram

7. Implementation and Results

This section consists of the various implementation details and snapshots of the blockchain Application developed using the blockchain Framework.

7.1. Implementation Details

Blockchain and distributed ledgers have a bright future. As real-time, open-source and trusted platforms that securely transmit data and value, they can help banks not only reduce the cost of processing payments, but also create new products and services that can generate important new revenue streams.

Solidity: Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum. It was developed by Gavin Wood, Christian Reitwiessner, Alex Beregszaszi, Liana Husikyan, Yoichi Hirai and several former Ethereum core contributors to enable writing smart contracts on blockchain platforms such as Ethereum. Solidity is a statically-typed programming language designed for developing smart contracts that run on the EVM. Solidity is compiled to bytecode that is executable on the EVM. With Solidity, developers are able to write applications that implement self-enforcing business logic embodied in smart contracts, leaving a non-repudiable and authoritative record of transactions. Writing smart contracts in smart contract specific languages such as Solidity is referred to as easy (ostensibly for those who already have programming skills). As specified by Wood it is designed around the ECMAScript syntax to make it familiar for existing web developers; [citation needed] unlike ECMAScript it has static typing and variadic return types. Compared to other EVM-targeting languages of the time such as Serpent and Mutan, Solidity contained a number of important differences. Complex member variables for contracts including arbitrarily hierarchical mappings and structs were supported. Contracts support inheritance, including multiple inheritance with C3 linearization. An application binary interface (ABI) facilitating multiple type-safe functions within a single contract was also introduced (and later supported by Serpent). A documentation system for specifying a user-centric description of the ramifications of a method-call was also included in the proposal, known as "Natural Language Specification."

Web3.js Api: Web3.js is a collection of inbuilt libraries that help to communicate with local or remote ethereum nodes by using HTTP or Interprocess communication (IPC).Web3 is designed to work from both client and server side. We can consider a web3.js as a gateway between Ethereum blockchain and a smart contract. This can be considered as the most advanced js library available.In blockchain, es-pecially the ethereum is made of nodes that share the same copy of data. By setting a web3 provider in a web3.js will helps the code to understand which node we are going to handle our functions. We can host our own node as a provider. Mostly we use some third-party services that help to maintain nodes in order to provide Dapp services. Some of the main providers include- Infura, MetaMask. Infura is a way to access the ethereum node over Jason-RPC which we can access through their API.With infura we can maintain our ethereum blockchain without setting up and maintaining our own nodes. MetaMask is a web browser add-on which acts as a bridge between and helps to run the Ethereum DApps without running the Ethereum full node. Metamask allows you to manage your Ethereum accounts and private keys, and use these accounts to interact with contracts that are using Web3.js. Metamask uses the infura.io servers as the web3 provider, other than that it also gives their users to choose their own web3 provider.

Truffle framework: Truffle is a development environment, a testing framework and a crypto asset pipeline in one for development in Solidity programming language. [1] The framework can build Distributed Apps (DApps), compile Smart Contracts, deploy Smart Contracts, and inject Smart contracts and DApps into a web app, and can create front-end for DApps and test them. Truffle framework has three main components named Truffle, Ganache, and Drizzle. Truffle Suite is a development environment based on Ethereum Blockchain, used to develop DApps (Distributed Applications). Truffle is a one-stop solution for building DApps: Compiling Contracts, Deploying Contracts, Injecting it into a web app, Creating front-end for DApps and Testing.

Ganache local blockchain: Ganache is a personal blockchain for Ethereum development you can use to

deploy contracts, develop your applications, and run tests. It is available as both a desktop application as well as a command-line tool (formerly known as the TestRPC). Ganache is available for Windows, Mac, and Linux.Ganache. Ganache is a personal blockchain that allows developers to create smart contracts, dApps, and test software that is available as a desktop application and command-line tool for Windows, Mac, and Linux.

Interactive Objects: The interactive objects explorer provides the user with the various interactive objects to interact with and consume knowledge through the touch based interaction. This is implemented using the FLASH HTML support for mobile devices. The framework app lists the HTML interactive files stored on the SD card. The user can then select between those for learning. When a selection is made the HTML code triggers the respective SWF file and the interactive object is displayed. User can then interact using the touch and gain knowledge.

8. Technical Specification

In this section we will discuss the advantages and limitations of the blockchain. We will also go through the applications of the framework and have a brief study about the technical requirements.

8.1. Advantages

Most blockchains are designed as a decentralized database that functions as a distributed digital ledger. These blockchain ledgers record and store data in blocks, which are organized in a chronological sequence and are linked through cryptographic proofs. The creation of blockchain technology brought up many advantages in a variety of industries, providing increased security in trustless environments. However, its decentralized nature also brings some disadvantages. For instance, when compared to traditional centralized databases, blockchains present limited efficiency and require increased storage capacity.

Following are some more advantages of blockchain Framework:

Distributed: Since blockchain data is often stored in thousands of devices on a distributed network of nodes, the system and the data are highly resistant to technical failures and malicious attacks. Each network node is able to replicate and store a copy of the database and, because of this, there is no single point of failure: a single node going offline does not affect the availability or security of the network. In contrast, many conventional databases rely on a single or a few servers and are more vulnerable to technical failures and cyber-attacks.

Stability: Blocks are very unlikely to be reversed, meaning that once data has been registered into the blockchain, it is extremely difficult to remove or change it. This makes blockchain a great technology for storing financial records or any other data where an audit trail is required because every change is tracked and permanently recorded on a distributed and public ledger. For example, a business could use blockchain technology to prevent fraudulent behavior from its employees. In this scenario, the blockchain could provide a secure and stable record of all financial transactions that take place within the company. This would make it much harder for an employee to hide suspicious transactions.

Potential to be two way and multi-media: Video, powerpoint, podcasts, and quizes are all potential outputs to iPhone devices. This provides a great deal of exibility for mobile development.

Trustless system: In most traditional payment systems, transactions are not only dependent on the two parties involved, but also on an intermediary - such as a bank, credit card company, or payment provider. When using blockchain technology, this is no longer necessary because the distributed network of nodes verify the transactions through a process known as mining. For this reason, Blockchain is often referred to as a 'trustless' system. Therefore, a blockchain system negates the risk of trusting a single organization and also reduces the overall costs and transactions fees by cutting out intermediaries and third parties.

8.2. Limitations

Reading the business or technical press you would think blockchain was the about-to-arrive answer to almost everything. That is to ignore some real problem areas, some technical, some environmental and some common sense. In this compilation, from multiple sources (see below), Enterprise Times attempts to raise some red flags which would-be blockchain adopters should reflect on. These may not destroy your faith in blockchain. They should give rise to thought. As noted economist Nouriel Roubini has written: “As for the underlying blockchain technology, there are still massive obstacles standing in its way, even if it has more potential than cryptocurrencies. Chief among them is that it lacks the kind of basic common and universal protocols that made the Internet universally accessible (TCP-IP, HTML, and so forth). More fundamentally, its promise of decentralized transactions with no intermediary authority amounts to an untested, Utopian pipedream. No wonder blockchain is ranked close to the peak of the hype cycle of technologies with inflated expectations.

8.3. Applications

The blockchain framework can be used in following areas:

Perhaps the most well-known blockchain application is being able to send and receive payments. Since blockchain technology has its beginnings in cryptocurrency, this makes sense. But, how exactly is this beneficial for small business owners? By using blockchain technology, you're able to transfer funds directly and securely to anyone you want in the world almost instantly and at ultra-low fees. That's because there aren't any intermediaries slowing down the transfer of funds between several banks and charging outrageous transaction fees.

"Smart contracts" are "self-automated computer programs that can carry out the terms of any contract," writes Chris DeRose in American Banker. In a nutshell "it is a financial security held in escrow by a network that is routed to recipients based on future events, and computer code." With "smart contracts" businesses will be able to bypass regulations and "lower the costs for a subset of our most common financial transactions." Additionally, these contracts will be unbreakable.

Cloud storage will be another application that businesses can take advantage of Storj, company that's using the blockchain to provide users with affordable, fast, and secure cloud storage. While talking to VentureBeat Storj founder Shawn Wilkinson said that, "Simply using excess hard drive space, users could store the traditional cloud 300 times over," much like how you can rent out a room on Airbnb. Wilkinson added, "Considering the world spends $22 billion + on cloud storage alone, this could open a revenue stream for average users, while significantly reducing the cost to store data for companies and personal users."

Blockchain technology offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner," says Rosic. "Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain-based authentication systems are based on irrefutable identity verification using digital signatures based on public key cryptography.

8.4. Hardware Requirements

AMD/Intel Processor

2GB RAM for application development Min. 16 GB Hard Disk

8.5. Software Requirements

HTML5

Ethereum Virtual machine (EVM) Java

XML

8.6. Mathematical Model

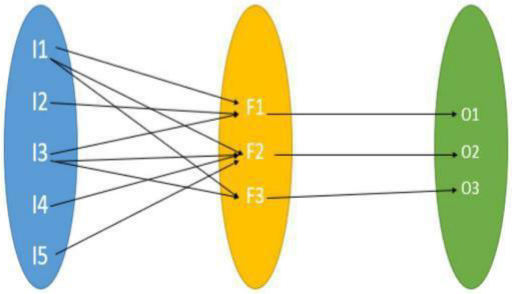
System Description :

System ={ I, F, O}
Where,
I = Input to the System,
F = Function of the System,
O = Output From the System.

I = {I1, I2, I3, I4, I5,}
Where,
I1 = Account No. Sender(User1),
I2 = Account No. Receiver(User2),
I3 = Account Holder Name,
I4 = Current Balance,
I5 = Account Type,

F = {F1, F2, F3,}
Where,
F1 = transferMoney() ,
F2 = cashWithdraw(),
F3 = balanceCheck(),

O = {O1, O2, O3, O4, O5, O6}
Where,
O1 = transfer Success or fail and balance updating,
O2 = balance reduce and update,
O3 = get user current balance ,



9. Conclusion

Information technology has become a critical innovation in almost every industry. Those institutions or teams that can use technology correctly and effectively play a major role in disrupting the status in a leadership position. Those that don't keep up with technology generally do not survive. We think the Blockchain technology as a catalyst for emerging use cases in the financial and nonfinancial industries such as industrial manufacturing, supply chain, and banking. Blockchain can play a pivotal role in transforming the digitization of industries and applications by enabling secure trust frameworks, creating agile value chain production, and tighter integration with technologies such as cloud computing, and IoT. In producing a cloud-based application called banking, the researchers have demonstrated the capability to apply professional engineering principles, combined with a DevOps approach to iterative development and management, and integration of cyber security, distributed computing, and Block-chain technologies. We feel banking is one of many examples that demonstrate the transformative capability of Blockchain.

10. Bibliography

[1] S. Nakamoto, \Bitcoin: A Peer-to-Peer Electronic Cash System," Www.Bitcoin.Org, p. 9, 2008.

[2] S. Sargolzaei, B. Amaba, M. Abdelghani, and A. Sargolzaei, “Cloudbased Smart Health-care Platform to tackle Chronic Disease," vol.4863, no. August, pp. 30-32, 2016.

[3] S. Underwood, “Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp.15-17, 2016.

[4] B. Libert, M. Beck, and J. Wind, \How blockchain technology will disrupt financial services firms," Knowledge@Wharton, pp. 2-7, 2016.

[5] G. Engaged, J. Tobe, G. Your, C. Computing, C. Dellorso, E. Apps, E. Reggie, R. Coughlan, and M. S. Fernandes, “Annual Conference - May 6-7, 2013-Kingsmill Resort ` The Value of Values : Linking Strategy and Decision Making "- 2013 Annual Conference Educational Sessions," 2013.

[6] W. E. Summary and S. Plants, \Power and the Industrial Internet of Things (IIoT)," no. January, pp. 1-14, 2015.

[7] M. Rosenfeld, \Multi-signature addresses," Bitcoin StackExchange, 2014. [Online]. Available: http://bitcoin.stackexchange.com/questions/3718/ what-are-multisignature- transactions.