Project Blockchain

Distributed Architectures and Programming

ISEP

January 2019

Bharath Reddy Nagasetty
60027
Kristoffer Ek
60013
Emb Wang
60035
Filip Galysz
60015

Abstract

Originally devised for the digital currency, blockchain represents an innovation in information registration and distribution. Transactions are broadcast, and every node is creating their own updated version of events. It is this difference that makes blockchain technology so useful. Being used as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks.

International money transfer services can benefit from blockchain technology to provide seamless real-time payment mechanism to SME population who need it the most. The current correspondent banking model and existing protocols are experiencing slow death as fintechs have unbundled these age-old financial services and the technologies like blockchain, cryptography, big data, and AI are fuelling fast adoption of new payment products by retail and commercial consumers alike as it addresses their main concerns of cybersecurity, and privacy and at the same time providing them with products that are intuitive, rich in content, and relevant to their needs.

Although, a little late to the game, banks have distinct advantages over startup fintechs in managing risk and providing liquidity for international payments, using existing AML/KYC frameworks and pursuing collaborative approach with other banks by adopting a homogenous blockchain platform, especially for underbanked/unbanked SME global population. The innovative service can provide a much-needed blueprint for worldwide adoption of payment platform through cooperation among central banks, IMF and regulators.

Executive Summary

The main objective of the project is to make a decentralized blockchain bank application for the future to eliminate the tampering of the ledger entries and make an application available to all and to upgrade the existing national and international idea in the field of blockchain and to set up these and benchmarks for future applications. The result is intended to facilitate an awareness about the growing trend of blockchain and its different currencies.

The current Money Transfer services for 245 million underbanked and unbanked SMEs worldwide are costly and cumbersome, opaque, slow as transactions are routed through many banks before they reach their recepients, causing delays and incurring fees. These shortcomings arise mainly from technology, regulation, and market structure.

The Blockchain (or distributed ledger technology) is a hot topic for discussion - it has the potential to revolutionise domestic and international transactions. The Blockchain is a public ledger of all the Bitcoin transactions, which continues to grow exponentially. Blockchain allows parties to transact securely in the absence of a third party intermediary and it is clear that some businesses recognise the potential savings connected to Blockchain or other distributed ledger technology.

Thousands of computers around the world are connected to the Blockchain, each holding a copy of the Blockchain history record. There is no official copy and no computer is seen as more valid than another - they each mutually verify the ledger and there is no centralised authority (such as a government or a bank). This decentralization is one of the revolutionary aspects of the technology.

The following tasks formed the core of the project:

1. To establish a distributed ledger for storing the transactions safe and securely where no alteration can be made to them once they are committed.

2. To identify the best software which can contribute to the building of ledger and analyzing them and scaling them to suit to the requirements of the project.
3. To build a smart contract container which can hold all the data logics which forms the backbone of the bank application.
4. To develop a design for the framework which meet the quality, standards and benchmarks and identifying the key aspects, type and level of detail of these benchmarks and standards.

Various methods were used for making the report. Firstly, the team members were allocated individual tasks and all the information was gathered and a backbone structure was made so as to how to use Hyperledger Framework for our application. Node.js was used to construct various scripts which included the functionality and working of the blockchain Explorer. Smart contracts were programmed in Go language and a transaction flow diagram was made and was evaluated with the actual working model.

Although it is hard to master the skill the blockchain and use it in the field of banking sector, besides the team managed to form a successful working model keeping the constraints in the mind which can be used for further development and improvement of the current model.

Table of contents

1.Introduction

1.1 Project introduction

The blockchain technology is a hot topic around the world these days, yet for many, the technology remains an elusive concept. This project aims to introduce the reader to the blockchain technology as well as to examine how one can implement a decentralized bank service using Hyperledger's smart contracts and distributed ledger technology.

1.2 What is blockchain technology?

An ordinary digital backbone is similar to the highly protected and centralized databases that governments or banks or insurance companies keep today. Control of centralized databases rests with their owners, including the management of updates, access and protecting against cyber-threats.

However, the distributed database created by blockchain technology has a fundamentally different digital backbone. This is also the most distinct and important feature of blockchain technology. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet.

Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology. Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. The blockchain is considered a type of payment rail. Bitcoin has been called "digital gold," and for a good reason. To date, the total value of the currency is close to $112 billion US. And blockchains can make other types of digital value.

Transactions are broadcast, and every node is creating their own updated version of events. It is this difference that makes blockchain technology so useful – It represents an innovation in information registration and distribution that eliminates the need for a trusted party to facilitate digital relationships. Yet, blockchain technology, for all its merits, is not a new technology.

Rather, it is a combination of proven technologies applied in a new way. It was the particular orchestration of three technologies (the Internet, private key cryptography and a protocol governing incentivization) that made bitcoin creator Satoshi Nakamoto's idea so useful.

Blockchains are built from 3 technologies		
1. Private Key Cryptography	2. P2P Network	3. Program (the blockchain's protocol)
Cash vs. Plastic	Tree falls in a forest	Tragedy of the commons
Identity	System of Record	Platform

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value", said Don & Alex Tapscott, authors of Blockchain Revolution.

1.3 What is Blockchain?

Using as a distributed ledger, a blockchain 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 a consensus of the network majority. Although blockchain records are not unalterable, blockchains 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 blockchain.

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 blockchain, 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.

Decentralization

By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad-hoc message passing and distributed networking.

Openness

Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view.

1.4 Public blockchain VS Private blockchain

Public blockchains

A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol). Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm. Some of the largest, most known public blockchains are Bitcoin and Ethereum.

Private blockchains

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

2.Method

2.1 Workflow

The project group consisted of 4 students whom all had different backgrounds and experience working with blockchain technology. At the start of the project, a git repository was set up to ease collaboration on the application. It was also decided that a distributed ledger technology (DLT) platform called Hyperledger Fabric should be used. The team members then worked iteratively on various parts of the application until it reached the set-out goal.

2.2 Hyperledger Fabric

Hyperledger Fabric is a permissioned Blockchain infrastructure, originally contributed by IBM and Digital Asset, providing a modular architecture with a delineation of roles between the nodes in the infrastructure, execution of Smart Contracts (called "chaincode" in Fabric) and configurable consensus and membership services. A Fabric Network comprises "Peer nodes", which execute chaincode, access ledger data, endorse transactions and interface with applications. End users then invoke chaincode through a client-side application that interfaces with a network peer. Chaincode runs network transactions, which if validated, are appended to the shared ledger and modify world state. "Orderer nodes" which ensure the consistency of the Blockchain and deliver the endorsed transactions to the peers of the network, and MSP services, generally implemented as a Certificate Authority, managing X.509 certificates which are used to authenticate member identity and roles.

2.3 Hyperledger Explorer

Hyperledger Explorer is a Nodejs based web app which runs on Node/ExpressJS with MySQL as the backend database. It provides details related Fabric blockchain network (channels) based on configuration provided in the file, blockchain_explorer/config.json.

2.4 Application

It was decided that the business logic, i.e. the chaincode, should be implemented using Golang. Furthermore, the client-side application should consist of multiple javascript files that all interfaces the network via the fabric library. Each file is a proof-of-concept of some functionality, such as create a customer or perform a transaction.

2.5 Prerequisites & Transaction Flow

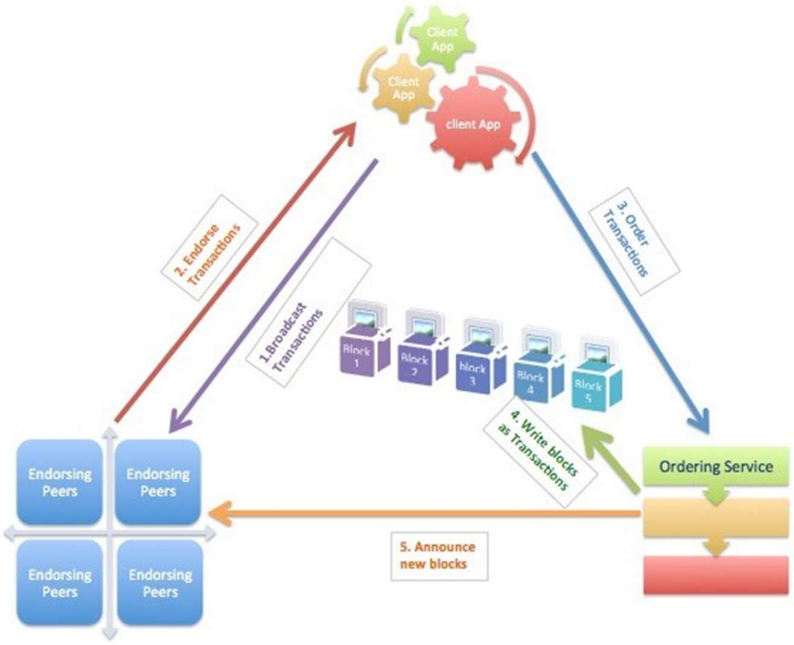
Prerequisites

In order to run the application, one needs to have all dependencies installed. These are for example Docker, which we use in order to run the network's peers in their own containers. NodeJS is used to run the client-side javascript application as well as the Hyperledger Blockchain Explorer. The MySQL dependency is due to the fact that the blockchain explorer uses it as the back-end database.

Transaction Flow

- Transaction requests are proposed by a client. The client must be connected to the required number of peers according to the endorsement policy. A proposed Transaction is forwarded to Peers for Endorsement.
- Each endorsing peer simulates and validates the transaction. Peers reply with their Endorsement and certificate if they agree that the transaction is permitted.
- The client receives results from different Peers and can thus verify agreement among the Peers. Upon verification, the client forwards the transaction to the OS.
- Determining a well-ordered sequence of transactions is the task of the Ordering Service (OS). The OS generates transaction blocks containing validated transactions in the order they are deemed to have occurred, writes them to the

ledger and then broadcasts them to all peers that a new set of blocks are now available on the ledger.



2.6 Money Transfer Network Setup

For our payment network, we will setup peers, one orderer service, CA authority service for certificate issuance and verification and one channel on which our peers will communicate.

Three representative banks Each one with the domicile country's currency reserves. These reserves are required because one of the competitive advantage we have considered is for banks to provide liquidity and thus manage risk.
Each bank also has customer accounts. When customers make payments to other customers, it is assumed that the payments will originate in the domiciled currency.

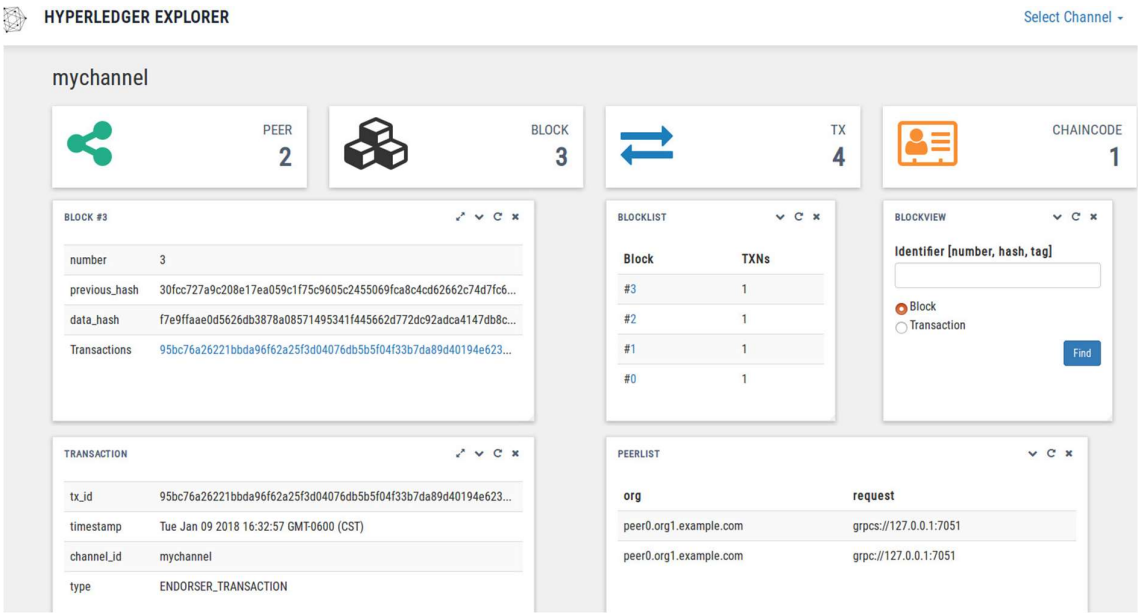
For e.g., US customer sending payments in USD to UK customer will have respective account debited, respective bank's reserves depleted and UK customer's account will be

credited with GBP after conversion and UK bank's reserves will be increased since they are receiving GBPs.

During the setup, forex pairs are populated. This is for the demo purposes only since the forex will be ideally retrieved in real time and perhaps can be provided as an input to the smart contract by the clients or through a forex backend of the banks.

We are setting up only one channel and all the banks in the network will subscribe to it. In real scenarios, consider setting up separate channels among group of banks to protect privacy of transactions for competitive purposes.

3.Results



This is the the complete developed UI for the bank application. It is based on the blockchain explorer provided by the hyperledger framework.

A successful blockchain bank application was developed using Hyperledger Fabric and using the chain code which is written in Go language, a popular language which is used to code and implement distributed applications in the Hyperledger framework. As the working environment is completely new to the team various problems were encountered while fabrication of the application.

The team has fulfilled the aim of the creating an application which can be used in the banking sector transfer funds across the countries ensuring the safety and security of the transfer and eliminating the need of intermediate banks. Although it eliminates the middleman it does take time in processing the transactions when applied on a larger scale.

Everything in reality has a few pros and cons. The hyperledger fabric has its own ledger which consists of the total information about the transactions and its hashes and it is used for permissioned blockchains where a person with the authority certificate can only make transaction unlike the bitcoin blockchain. Fabric offers a modular

architecture where developers can create plug in components which come in handy. Channels in Fabric provide a data partitioning capability that achieves the physical separation of sensitive data.

As the Hyperledger Fabric is new in the global market there is a lack of proven cases and inadequate number of skilled programmers able to use it. The amount of data that can be stored in a ledger is limited. As it is limited to only chain code it creates a bottleneck for the new users to program it. The team faced a lot of challenges in executing the application on the local machines as the working completely dependent on the architectures of the local ones. The final limitations is takes a lot of time for completion and a single error can cause the havoc to the user.

4.Conclusion

Blockchain a future technology although being hard to learn and most trending now a days the question is remains unsolved how it has to be implemented in precise. The database era is being replaced by blockchain since modification of transaction can be done after committing the transactions.The blockchain application presented here solves the problem of intermediary bank ensuring fast and secure transaction which are P2P based.

However it will take time, money and combined effort of many skilled programmers to deploy it on a global scale.The design perfectly matched the expectations and was stable when tested against different environments. The popular theory which stated that databases form the backbone of banking sector was proved wrong and alternative Hyperledger Platform was used.

5.Bibliography

- https://www.fincen.gov
- https://www.occ.gov/topics/responsible-innovation/comments/recommendations-decisions-for-implementing-a-responsible-innovation-framework.pdf
- https://www.r3.com/about/
- http://hyperledgerfabric.readthedocs.io/en/release/channels.html
- http://slideplayer.com/slide/10071927
- https://www.theclearinghouse.org/media/files/payco/files/pmpg_dodd_frank_1073_whitepaper_sep 2013 final.pdf
- https://www.usitc.gov/publications/332/pub4189.pdf
- https://ibm.com/ Hyperledger Fabric