Credit-Union-on-Blockchain---A-new-financial-Cooperative-system-based-Permissioned-Blockchain

Abstract:

Everyone needs help at one point or another. The same is true for financial help, for this reason most people rely on loans to satisfy their financial needs. “Loans to Private Sector in the United States averaged 619.94 USD Billion from 1950 until 2020, reaching an all time high of 2364.08 USD Billion in August of 2019 and a record low of 13.65 USD Billion in January of 1950”Trading Economics, To satisfy this growing demand of loan, banks and Credit Union offer financial services such as saving accounts, loans and the possibility of transferring money one to another. This project focuses on developing a web blockchain application which allows individuals to create or join a group where they will be able to save money, borrow to/from one another, while keeping track of every transaction without a third party. We will build a digital web application with a database built on permissioned blockchain using smart contracts. “Permissioned blockchain restricts the actors who can contribute to the consensus of the system state. … secure the interactions among a group of entities that have a common goal but which do not fully trust each other, such as businesses that exchange funds (finance), goods (supply chain), or information (public service). By relying on the identities of the peers, a permissioned blockchain can use traditional Byzantine-fault tolerant (BFT), RAFT, or Paxos consensus.”Guo, C., Ma, S., Wang, H., Cheng, S., & Wang, basing our web application database on permissioned blockchain gives the security, transparency and transability to the loan system.

1. **Introduction**

People will always need funds when starting their own business as a new auto repair shop or haircut shop, even when they are starting a new project like a new kitchen design or buying a new car, and emergency also is a perfect example where they will likely need funds. But they always rely on the tedious loan process offered by bank and financial corporations such as Credit Union. And if they are lucky enough they will get those funds with an enormous interest rate. With the advance of social media and social ap services people are connected more than the early century. In fact, we have more friends online than in real life. Even though you cannot rely on your online friend for your issue, that necessitates an amount of money that you cannot afford by yourself.

Paypal understood the benefit of adding a new value to social networks by creating a group of saving accounts into their digital application offering a group of people the chance to support one another by saving money together for a matter that regards one of them. But although the service is a huge step on social support, it is nevertheless insufficient in the case to benefit the other members of that social network. Because, we all know social aid is better when it is an investment. More precisely, by making the amount saved by the social network as a loan to whoever wants it to resolve his issue it will be more beneficial to everyone in the network. Aslo, the average american save into their savings account does not go over $20000 which is less than 50 percent of what they earn ($44000) per year. This is due to the fact that american rely on rely on financial institutions to manage their assets. Plus they rely on their own assets or bank loans to solve their common financial issues.

This paper is resolve to show how the use of social network and fintech in the issue of social support and is summarized as follow:

* We discuss the blockchain subject.
* We discuss what is a Permissioned Blockchain
* We propose a digital application design from a Credit Union template business logic and based on permissioned blockchain.
* We propose the design of the structure of the association of people saving money

1. **Blockchain.**

This paper discusses the design and implementation of a digital application which technology is based on permissioned blockchain. Let's discuss what blockchain actually is, then how it works and finally what is the advantage of using permissioned blockchain over permissionless ones.

Blockchain is Distributed Ledger Technology where digital assets are unalterable, making the ledger impossible to be modified, they are transparent, every member of the ledger has the record of every transaction. These assets are transact through the use of decentralization and cryptographic hashing. Since its creation Blockchain has been potentially used in more than 8 sectors such as:

* Payment processing and money transfers
* Monitor supply chains
* Digital IDs
* Data sharing
* Copyright and royalty protection
* Digital voting
* Real estate, land and auto title transfers

So it is understandable to know how it works. Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger. It is composed of blocks, nodes and miners.

**Blocks**

Every chain consists of multiple blocks and each block has three basic elements:

The data in the block.

A 32-bit whole number called a nonce. The nonce is randomly generated when a block is created, which then generates a block header hash.

The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

**Miners**

Miners create new blocks on the chain through a process called mining.

In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.

When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

**Nodes**

One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning.

Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that shows their transactions.

Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scalability of trust via technology.

There are two principal kinds of Blockchain Technology. A permissionless Blockchain and a permissioned blockchain. The permissioned blockchain will be the object of our research, they are working by the use of smart contracts. Smart contracts enabled in DLT are virtual agreements encoded on the network that are automatically executed based on logical conditions. The automatic execution is an important attribute for smart contracts . Institutions also focus on the data security and privacy of smart contracts in DLT. Platforms running user-defined smart contracts and executing user-supplied transactions on their objects are also carried out. In recent years, the financial industry is also moving towards expressing financial agreements via financial smart contracts, which serves as precise notations for expressing financial agreements among parties. Now let's look more about the permissioned blockchain.

1. **Permissioned Blockchain**

Permissioned blockchains are blockchain networks that require access to be part of. In these blockchain types, a control layer runs on top of the blockchain that governs the actions performed by the allowed participants. Privacy is a core in permissioned blockchain; Depending upon the permissioned network (e.g., in Corda), only selected participants get to participate in a given transaction for a private permissioned ledger. Data is shared with selective nodes based on the smart-contract logic on the ledger. In the consensus mechanism, Private permissioned ledgers use more efficient consensus algorithms. Some of the ledgers also allow the use of more than one consensus algorithm within the same network. Permissioned blockchain is more performant for enterprise applications due to a closed network with fewer number of nodes where participants are already known. There is the capability to add nodes and services on demand, which is a much more practical approach to any business solution.

Hyperledger Fabric is one of the most used permissioned blockchain. Datas in the ledger are updated through the use of smart contracts packed into chaincode applications. Hyperledger Fabric is intended as a foundation for developing applications or solutions with a modular architecture. Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play. Its modular and versatile design satisfies a broad range of industry use cases. It offers a unique approach to consensus that enables performance at scale while preserving privacy. Typical Hyperledger fabric network design is made of:

* Ordering Service: Because Fabric’s design relies on deterministic consensus algorithms, any block a peer validates as generated by the ordering service is guaranteed to be final and correct. Ledgers cannot fork the way they do in many other distributed blockchains.
* Peer: A blockchain network is composed primarily of a set of peer nodes (or, simply, peers). Peers are a fundamental element of the network because they host ledgers and smart contracts. Recall that a ledger immutably records all the transactions generated by smart contracts (which in Hyperledger Fabric are contained in a chaincode, more on this later). Smart contracts and ledgers are used to encapsulate the shared processes and shared information in a network, respectively. These aspects of a peer make them a good starting point to understand a Fabric network.
* Endorser: for a transaction to be valid, peers with endorsement qualificalifications have to endorse the request from the client application.
* Membership Service Provider(MSP):
* Ledger: Is a key concept in Hyperledger Fabric; it stores important factual information about business objects; both the current value of the attributes of the objects, and the history of transactions that resulted in these current values
* Smart Contract:

Before businesses can transact with each other, they must define a common set of contracts covering common terms, data, rules, concept definitions, and processes. Taken together, these contracts lay out the business model that govern all of the interactions between transacting parties.

* Private data: In cases where a group of organizations on a channel need to keep data private from other organizations on that channel, they have the option to create a new channel comprising just the organizations who need access to the data. However, creating separate channels in each of these cases creates additional administrative overhead (maintaining chaincode versions, policies, MSPs, etc), and doesn’t allow for use cases in which you want all channel participants to see a transaction while keeping a portion of the data private.
* Chaincode:

The smart contracts defined within a chaincode encode the domain dependent rules for a business process agreed between a set of blockchain organizations. However, a chaincode can also define low-level program code which corresponds to domain independent system interactions, unrelated to these smart contracts for business processes.

1. **Developing The Digital Applications**

In this section, we will discuss how we develop a client application and smart contract to solve the business problem using Hyperledger Fabric.

This Section follows a typical software development lifecycle. It starts with business requirements, and then covers all the major technical activities required to develop an application and smart contract to meet these requirements.

**4.1.1. The Scenario**

In this topic, We are going to describe a business scenario involving one organization,a bank and an individual who uses the digital application of our study to send, save and loan money. We are going to use the scenario to outline requirements for the development of web application applications and smart contracts used by the participants.

**MoneyNet network**

MoneyNet is a Hyperledger fabric network that allows suitably authorized participants to send money to one another, save into their group account and loan.

Let’s see how users use MoneyNet transact into the network.

**Introducing the actors**

Steve is a young student studying at Quinsigamond Community College. Steve has two part time jobs and makes an average of $40000 every year. Recently, Steve noticed that he can save an average of $10000 every but still with an APY of 0.09 he can only benefit $9 every year from his savings account. He then decided to create his own personal financial institution with 11 others of his classmates. However, opening a financial institution in the United State requires some resources that Steve does not possess. Steve, nevertheless, finds it useful to save money with his classmate into a personal bank account. The bank then issues commercial papers and gives them to Steve’s group as representation of their money saved. Now Steve’s group possesses the MoneyNet paper.

David One of Steve’s friends but not a member in Steve’s group needs money to open his hair cut shop. He then goes to Steve to ask for Loan.

**Loan Process**

To operate all the transactions Steve and members of his group write the smart contract and install it to their node.

David connects to the application through one of the peer gateway and requests a loan depending on the group policy, the loan is approved.

The bank connects to the application, retrieves David's information from the request and sends money into David’s personal bank account.

After a given period David settles the loan with interest and Steve and members of his group will have an amount of their asset increase depending on their percentage or the money they saved.