THE UNIVERSITY OF
MELBOURNE

School of Computing and Information Systems
University of Melbourne

The Prototype of Order Tracking & Certification Application Leveraging Blockchain Technology

Kaiquan Shi, 906555, kaiquans@student.unimelb.edu.au
Tao Jin, 827872, tjin2@student.unimelb.edu.au
Yubing Yang, 883877, yubingy@student.unimelb.edu.au

Supervisor: Prof. Richard Sinnott, rsinnott@unimelb.edu.au
COMP90055 2019 SM1

Abstract

The task of this project is to build a decentralized application that can help customers that allows customers to check the source of the goods they received. Traditional web applications are vulnerable to attacks, so that the authenticity and integrity of data cannot be effectively guaranteed. The introduction of blockchain technology can solve this problem because the blockchain effectively prevents data from being deleted, and the editing of data is recorded by each node in the peer-to-peer structure.In this project, we implemented a decentralized application using product data from Capral Ltd. These data include product title, short description, categories, product certificates, etc. Manufacturers distributed in different locations around the world will send the corresponding data input blockchain when order is shipped, and update the logistics information of the product in the blockchain. Whenever a new entry is generated, the corresponding link and QR code are also generated, which helps the customer to track the source of the product.

Declaration

This thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person where due reference is not made in the text.
We have received clearance for this research from the University's Ethics Committee and have submitted all required data to the Department.

Acknowledgement

This paper was completed under the direction of Dr Richard Sinnott. Dr Richard Sinnott's profound expertise and rigorous academic spirit have had a profound impact on us. From the selection of the subject to the final completion of the project, Dr Richard Sinnott has always given us careful guidance. Here, we would like to express our sincere gratitude to Dr Richard Sinnott!

We also received great care and help from friends and family in life and learning, thank you!

Table of contains

Table of figures

1. Introduction

Blockchain is a very popular emerging technology. It is a combination of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm.

A blockchain is essentially a decentralized database. It is a chained data structure in which data blocks are sequentially connected in chronological order, and cryptographically guaranteed non-tamperable and unforgettable distributed ledgers. Each block contains information that needs to be protected, associated information with other blocks, and information that supports data validation.

Blockchain technology is a new distributed infrastructure and computing method. It uses blockchain data structure to verify and store data, use distributed node consensus algorithm to generate and update data, and use cryptography to ensure data transmission. And access security, using smart contracts consisting of automated script code to program and manipulate data.

2. Background

We live in a digital age. Many information needs to be transmitted and stored in the cloud through the network. This promotes information sharing and production automation. But on the other hand, it also brings hidden dangers of information security. Some individuals and organizations add, modify, or delete relevant information in a network-based shared database for the benefit of themselves. For example, in the product supply chain, some distributors falsify the logistics information of the products in order to obtain greater benefits, they confused the identity of the upstream manufacturers. This makes it impossible for the customer to confirm whether the product in hand is from a manufacturer that is consistent with the order, or whether the product is in line with expectations from production to processing.

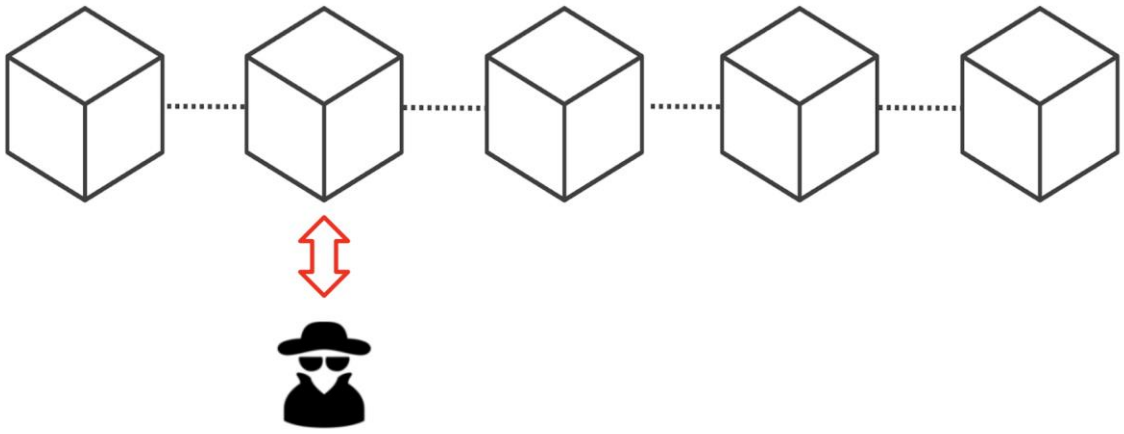
In this model, the main reason for the database to be attacked is that it adopts a centralized structure, and the original data will be overwritten after the data is changed, so it cannot be verified.

Blockchain technology just happens to avoid such threats. First, the blockchain uses a peer-to-peer network structure, and each user who joins the blockchain has a complete account book. Second, the data that has been saved in the blockchain cannot be changed, which makes the history information of each data update completely recorded.

3. Technology

In a valid blockchain, each block contains the hash value of previous block, some data, and the hash value of the current block. Bitcoin is an important application of the blockchain, in which each block stores transaction information. However, the data that can be saved in the blockchain is not limited to this. Similar to traditional databases, blockchains can hold different types of data under different requirements. For example,

in a blockchain used for supply chain management, the data in the blocks should be some information that supports order validation.The hash values are calculated by hash functions it's always unique, so it can be used to identify a block just as a fingerprint. Once the data inside the block has been changed, its hash value will also be changed. As a consequence, the hashing scheme can help us to detect modifications.



Let's take an example in the figure. Here we have a chain of 5 blocks, each block has a hash and the hash of the previous block. Temparing with the second block causes the hash of the block to change as well. When the hash value in a block is modified, the previous hash value stored in the subsequent block will no longer match it, which will cause the subsequent block to become invalid. In turn, all the block after the modificated block will be invalid.

However, the hash function is not sufficient to make the blockchain completely reliable. Computers nowadays are very powerful and can process massive data in a short time frame. If the attacker modifies the information in a block and recalculates the hash values of all the subsequent blocks, the blockchain will remain valid. In order to avoid this kind of attack, the blockchain also introduces a proof-of-work mechanism, which makes the calculation process of hash value significantly increase, thus slowing down the speed of generating new blocks. In Bitcoins blockchain for example: when you want to add a new block, it will take you about ten minutes to calculate the have value because of the proof-of-work mechanism. The chain of hash values and the scheme of proof-of-work makes blockchain very safe. Because when an attacker wants to change the data in a block, it takes a lot of time to recalculate the hash values in subsequent blocks.

In addition, unlike the centralized database, the blockchain uses a peer-to-peer(P2P) network structure, which makes the blockchain more secure.The blockchain is open to all users, which means that when a new user joins the network, he will get a full copy of the data already in all the blockchains. Each update of the blockchain will be processed through the smart contract mechanism and stored in each node of the P2P network.

So, if an attacker wants to change the data in the blockchain, he needs to get access to at least 50% of the nodes in the P2P network, recalculate the hash function with the delay of proof-of-work mechanism. Only then the modified data will be valid in the tampered blockchain, but this is a task that is almost impossible to accomplish.

In this project, we developed a decentralised application(Dapp) to track the product information. A Dapp is a web application that utilizes blockchain technology. The front end of Dapp uses the same technology as traditional web applications. The main difference exists in the back end structure. Instead of Application programming interfaces(APIs) connecting to databases in traditional web application, there are Smart Contracts connecting to blockchains in Dapp.

4. Related work

1 blockchain product examples

Steem is an encrypted currency that circulates on the steemit platform. Steemit is a decentralized social media platform that motivates users to participate in creation through micropayments. Users also encourage creators by using Steem currency for micropayments, which allows content creators to publish articles on the blockchain platform to get direct benefits into reality.

Brave was created by JavaScript inventor Brendan Eich.People can use the Brave browser to watch ads and get BAT coins. The BAT coin is called the Basic Attention Token, which is equivalent to the bonus point that the browser member can sign in to sign in. However, it increases the liquidity.The Brave browser development team introduces very attractive incentives for users to watch ads that are 70% of total advertising revenue, which is billed monthly through BAT tokens. Brave's Token is used to motivate users to choose the right ads for them, and advertisers provide better advertising.

Bancor is a decentralized mobility network that allows users to use a simple web wallet, hold any tokens and convert them to any other token in the network, without the other party, to automatically calculate the price.

Bancor-compatible tokens are a new ERC20-compatible token on the Ethereum blockchain, thanks to its built-in features, making them an essentially tradable token. This feature is simple but far-reaching: you can have one token endorsed by another token or tokens, holding these endorsement tokens as a reserve at a ratio of 0 to 100%. In this way, the price of this token will be automatically set according to its supply, reserves, and ratio. The transaction does not require the participation of the second party.

Golem is one of the earliest generations of Ethernet applications. The token is GNT, which is a decentralized computer computing rental platform built on the Ethereum platform. Through the Golem platform, any user can become a power seller and renter. Whether you have an idle home computer or a few large data centers, you can join the Golem platform. The trading system based on Ethereum is applied to the Golem platform to settle the revenue of the computing provider and the cost of the computing user.

2 Differences between traditional bitcoin and ethereum

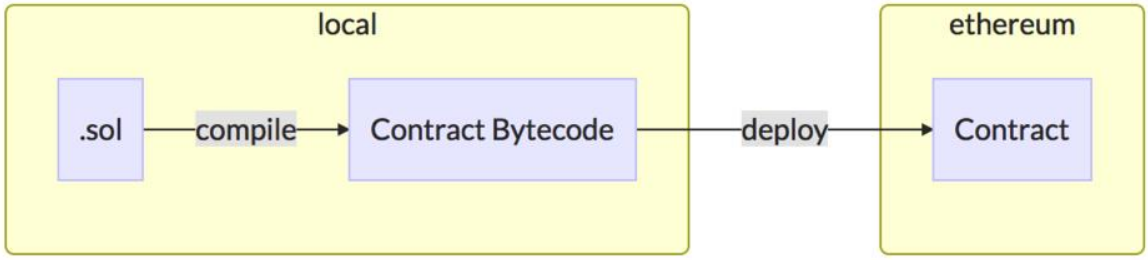
Bitcoin is a value storage tool designed to be a global, peer-to-peer, distributed, and transparent digital currency. In contrast, Ethereum's design provides an ecosystem for distributed applications and decentralized autonomous organizations (DAOs). Unlike most people's perceptions, Ethereum and Bitcoin have different goals. Ethereum focuses on making the blockchain more attractive to users, while Bitcoin is committed to changing finance industry.

Both Bitcoin and Ethereum are based on decentralized blockchain technology, but there are still many differences in the deep technical field. For the specific performance of decentralization, Bitcoin is mainly divided into three aspects: complete node decentralization, computational decentralization, and development decentralization. In contrast, the development process of Ethereum is completely centralized, although it can

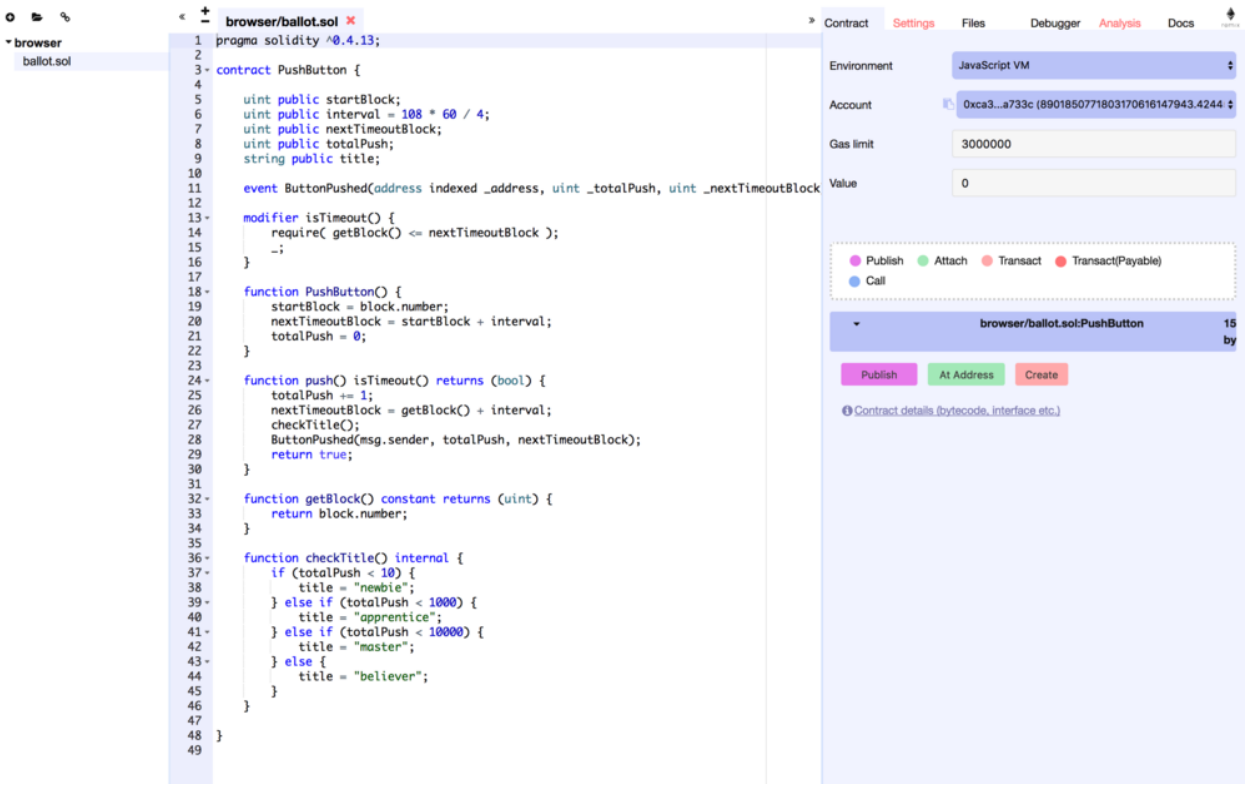
greatly improve efficiency, but it also makes it impossible to guarantee the security of its rules and is vulnerable to attack.
Bitcoin was originally designed as a decentralized cryptographic currency network for trading currency values. The main purpose of the Bitcoin blockchain is to provide trust support for these financial transactions.
Contrary to Bitcoin, Ethereum has been conceived as a decentralized application development platform since its first day, and its blockchain is designed to support the operation of decentralized applications.
Therefore, the design of Ethereum learned from the experience of Bitcoin and improved the shortcomings of Bitcoin. The difference between the two systems is that Ethereum's data processing is faster than Bitcoin, because the Ethereum system automatically applies to the terms and conditions of the contract once agreed.

3 smart contract
(1)The uniqueness of smart contracts
a whole alloy flow is easy
It's not easy for a typical application to integrate the golden stream. Smart contracts are extremely easy to integrate with the Golden Stream system (using Ethereum or a new token contract created by itself).
b Additional costs for deployment and subsequent writes
The general application needs to provide the URL for the user to download. The general web application also needs to run on the server. The developer needs to maintain the operation of the server to provide the service, which requires continuous cost (even if it is a free server or The web space is also absorbed by the manufacturer itself. After the program starts running, there is no additional cost other than maintaining the cost.
Smart contracts require a fee for deployment, which is distributed to those involved in transaction verification (mining). After the contract is successfully deployed, the contract is distributed as part of the unchangeable blockchain and is stored decentralized at nodes in Ethereum around the world. Therefore, after the smart contract is deployed, there is no need to provide maintenance costs on a regular basis, and there is no charge when querying static data that has been written into the blockchain. Only a small transaction fee is required each time a calculation is written or read through a smart contract.
C The cost of storing data is higher
A general application stores data on the local machine or server. When the data is needed, it is read from the local machine or the server. The smart contract stores the data in the blockchain. The time and cost required to store the data are relative to the cost. expensive. Fourth, after the deployment can not be changed, the general application can be modified by installing a new version of the program, the web application can also be achieved by deploying a new version of the program, and the

smart contract cannot be modified after being applied. Of course, smart developers have had the means to bypass the limitations of smart contract deployments that can't be changed by adding additional smart contracts.
(2) How to write a smart contract?
Smart contracts on Ethereum need to be written in solidity language.
After writing the solidity code (.sol), we need to compile (compile) the program code into the binary contiguous Contract ByteCode that EVM (Ethereum Virtual Machine) can read before deploying to Ethereum. Executed on the blockchain. Contracts deployed on the blockchain will have a Contract Address in the same format as the wallet address (address).



Smart contracts can be executed automatically after deployment. When a subsequent smart contract is called, the user can use the wallet address (owner account) of the deployment contract, or allow other wallet addresses to call this smart contract by the smart contract conditions written. Calling a smart contract is actually a transaction to this contract address, but the transaction is not just a token, but a call method provided by a smart contract.



5. Requirements analysis

(1) data analysis

The given excel table shows the basic information of capral products, including title, picture file number, short description, all_product_categories, created/updated time and so on.

(2) requirement

The goal of our project is to design a web app to meet the following requirements. The first one is that customers can search for any information they want to know about the products they have bought. For example, customers can find the detailed materials and created time in the app, even whether the product meets the Australian standard. Moreover, they can track the current location of the product and the time when they can get it.

(3) design schedule

Feb: Collect the knowledge and background about blockchain together. Analyze the data and requirement.

March: Build the basic architecture including blockchain, smart contract and so on.

April: Complete front-to-end system

May: Implementation of the web app and fix bugs.

6. Conclusion

As a cutting-edge technology, blockchain brings both chances and challenges to different fields. In this project, we use blockchain-based technology to construct a web app. Users can use this app to track, search and verify the capral product. Ethereum is a useful blockchain platform for developers and smart contracts provides the reliability. However, the project still has a lot to improve in the future. In conclusion, blockchain technology is used in more and more fields nowadays. It's meaningful to learn about it for everyone.

Reference

Appendix

Video Link: https://www.youtube.com/watch?v=-zSWo0IQH0g

Medium. (2019). *Top 5 Working Products in Blockchain (Updated — October 2018)*. [online] Available at: https://medium.com/theblock1/top-5-working-products-in-blockchain-updated-october-2018-9b18548bf8fc [Accessed 11 Jun. 2019].

Hajimirza,A. (2019). *Azure-Samples/blockchain*. [online] Available at: https://github.com/Azure-Samples/blockchain/tree/master/blockchain-workbench/application-and-smart-contract-samples [Accessed 11 Jun. 2019].

Munro, A. (2019). *Bitcoin vs Ethereum: A side-by-side comparison* | *finder.com.au*. [online] finder.com.au. Available at: https://www.finder.com.au/bitcoin-vs-ethereum [Accessed 11 Jun. 2019].