Blockchain Application for User Privacy in Online Transactions

Jingwei Wang 515030910619

May 27, 2018

Abstract

Despite an increasing focus on the privacy of online shopping and a growing expectation for protecting individual information, the private information of buyers is subject to data breaches inevitably in essence, the right to decide in the hands of Internet companies. Blockchain technology is an rising technology that enables data sharing in a decentralized and transactional way. In this report, I proposed a blockchain-based framework to insure an anonymous and secure system for a convenient onlinetransactions. The goals of this paper are to clarify how this framework could solve the privacy and security concerns.

I. Introduction

Security and privacy are the central issues for the acceptance of online transactions in particular and growth of the Internet market in general. Modern people have little privacy. "(Information) Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others"[1]. The location and moving tracks of modern people is always known when carrying a mobile phone. Using the credit cards for online shopping their shopping habits are also sold to when people can't imagine. Using static Internet Protocol (IP) addresses, cookies user's interesting topics can easily be discovered.

Confidentiality, authentication, integrity, and nonrepudiation are the four basic components for secure online transactions. Some methods have proposed to solve these problems but didn't focus on the key aspect, that there are centralized institutions, both public and private, have collected user's information as soon as user access their products. Individuals have little or no control over the data that is stored about them and how it is used. As we all know, these data are a valuable asset in our economy.

A blockchain is an append-only data structure that functions as a distributed ledger. This is accomplished by copying all the data on the blockchain across all nodes in the system. As a result of this redundancy, a blockchain is easily verifiable and has no single point of failure. Blockchains are created by having nodes in the system 'mine' blocks, or create additions to the structure using a hash of transactions that people have recorded on the blockchain. This structure makes blockchains immutable unless participating nodes with 51% of computation power on the blockchain choose to rewrite the chain. Both mining and storing so many copies of the same data does have its costs in computational power and storage, but they are necessary for a blockchain to be a completely decentralized, immutable system.

These kinds of systems have already emerged. *Bitcoin*[2], which allows users to transfer currency (bitcoins) securely without a centralized regulator, using a publicly verifiable open ledger (or blockchain). However, it doesn't make any sense. For connecting with buyer and expressing the shopping goods, user's address and mobile phone are exposed to the online store and express compa-

nies obviously. This framework illustrate that blockchains still have the potential to become a vital resource in trusted-computing.

II. Methods

This system is mainly base on the blockchain technique, but modified a lot.

i. node

Nodes in this system can be classfied into three typies, user nodes, intermediary nodes and merchant nodes(including merchants and express stations). Intermediary nodes are not mastered by any instructions. They act as an intermediary between user and merchants, providing service for users and protecting user privacy, such as offering a goods database to users.

ii. Transactions

A vital problem in decentralized transactions is the payee can't verify that one of the owners did not double-spend the coin. The only way to confirm the absence of a transaction is to be aware of all transactions. In previous blockchain system, transactions must be publicly announced. But in online shopping, user's name, address are private information which can't access by merchants.

In this system, a transaction in the blocks didn't contain the user and address information. There are some intermediary nodes to make transactions with users, which are not mastered by any instructions. Users will send their address and signature to these intermediary nodes privately and they will interact with merchants and express stations. Merchants only know the goods, next express station and the signature from users while express stations just know express number and the next express stations. Users split their address to several parts, that each path means a express station. Such as "Shanghai JiaoTong University, Minhang, Shanghai" will be split to "Shanghai JiaoTong University" express station, "Minhang" express station and "Shanghai" express station. Intermediary nodes will send "Minhang" express station, corresponding express number and a unique signature to "Shanghai" express station privately.

iii. Privacy

This system have no doubt to use a key pair, private key and public key. Public keys represent the unique identification in blockchain system to annoymize it real owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

In this system, a transaction isn't connected with public key of user directly. Via an intermediary node, merchants can just get a transaction request and user information are confused. This feature make sure the privacy of users because no one indeedly know the information of user.

III. implement

There is a simple demo code for this system. This code is thoroughly run in native, Although some files should be stored in intermediary nodes as a database. However, main features of this project have given.1

IV. Discussion

In this project, I proposed a system for online transactions with high anonymity based on the blockchain technique. It avoids merchant to access user information effectively and thereby protect user privacy. However, it's not total safe and anonymous, as blockchain have a lot of problem existing which this system didn't think over. Despite this, blockchain may not be a good technique under online shopping because its high power and storage costs and high transaction time delay.

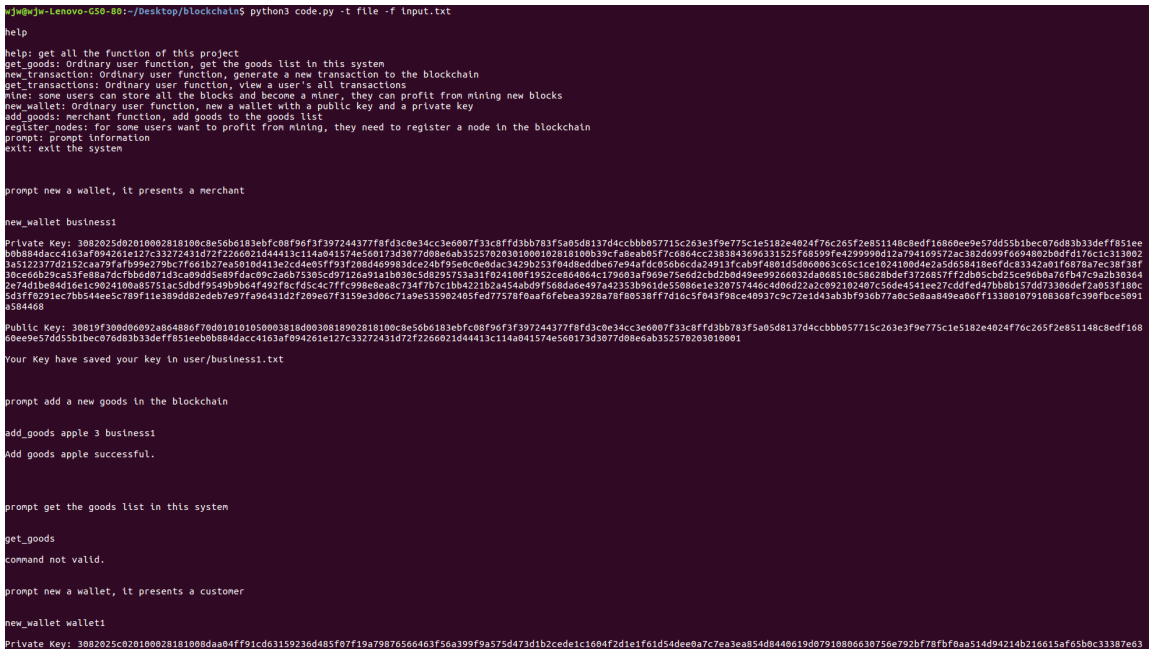

Figure 1: A demo run of my code. Basic functions like generating transactions, generating wallets, have realized

References

[1] A. Westin. Privacy and Freedom, Athenum, New York, 1967

[2] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008

[3] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283-297