

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 classified 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 Jiao-

Tong 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 annoyimize 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.

```

lsj@lsjw-Lenovo-G50-B0:~/Desktop/blockchain$ python3 code.py -t file -f input.txt
help
help: get all the function of this project
get_goods: Ordinary user function, get the goods list in this system
new_transaction: Ordinary user function, generate a new transaction to the blockchain
get_transactions: Ordinary user function, view a user's all transactions
mine: some users can store all the blocks and become a miner, they can profit from mining new blocks
new_wallet: Ordinary user function, new a wallet with a public key and a private key
add_goods: merchant function, add goods to the goods list
register_nodes: for some users want to profit from mining, they need to register a node in the blockchain
prompt: prompt information
exit: exit the system

prompt new a wallet, it presents a merchant
new_wallet business1
Private Key: 38828025d0010002818100c0e56b183ebfc08f96f397244377f8f3c0e34cc3e6007f33c8ffdbbb783f5a05d8137d4ccb057715c263e3f9e775c1e5182e4024f76c265f2e851148cedf16860e9e57d55b1bec076d83b33def851ee
b0b884dacc4163af094261e127c33272431d72f2266021d44413c114a041574e560173d3077d08eab35257020301000102818100b39cfac8eab05f7c6864cc2383843696331525f68599fe4299990d12a794109572ac382d699f6694802b0df4176c1c313002
3a512377d2152caa79fafb99e279bc7f661b27e85010d413e2cd4e05f93f708d469983dce24b95e8c0e0dac3429b253f04d8eddcb67e94afdc05b0cda24913fcb9f4801d5d060863c5c1ce1024100d4e2a5d658418e0fd8c83342a01f6878a7ec38f38f
38c46029c53f8887d6cf8b0871d2ca9d0e89f8ac09c2ad075380cd97126a911a3b38c5d82932331f024100f192c864064c19663a3969e75e6d2c0db0649e092f6832d086510c38628b0ef3726831ff0db05c4d2c5ce080a7f6847c9a2b33364
2e74d1be84d16e1c9024100a85751ac5dbdf9549b964f492f8cfd5c4c7f9c98e8e8c734f7b7c1bb4221b2a454abd9f58bdae49744233b961de55886e1e32075744c4d06d22ac092102407c5d6e4541ee27cd0fed47bb0b157d73306def2a053f180c
5d3ff0291ec7b544e5c789f11e389dd82edebe9f7f96431d2f209e67f3159e3d06c71a9e535902405fed77578f0aaf6f6eba3928a78f80538ff7d16c5f043f98ce40937c9c72e1d43ab3bf930b77a0c5e8aa849ea06ff133801079108368fc390fbc5091
a504468
Public Key: 38819f30d060092a864886f70dd01010500038180003818902818100c0e506183ebfc08f96f397244377f8f3c0e34cc3e6007f33c8ffdbbb783f5a05d8137d4ccb057715c263e3f9e775c1e5182e4024f76c265f2e851148cedf168
60e9e57d55b1bec076d83b33def851eeb0b884dacc4163af094261e127c33272431d72f2266021d44413c114a041574e560173d3077d08eab352570203010001
Your Key have saved your key in user/business1.txt

prompt add a new goods in the blockchain
add_goods apple 3 business1
add_goods apple successful.

prompt get the goods list in this system
get_goods
command not valid.

prompt new a wallet, it presents a customer
new_wallet wallet1
Private Key: 38828025c0201000281810080daa4ff91cd63159236d485f07f19a7987656463f5ea399f9a575d473d1e1f61d54de0a7c7ea3ea854d8446619d07910806630756e792bf78fbfaa514d94214b216615af65bc3387e63

```

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