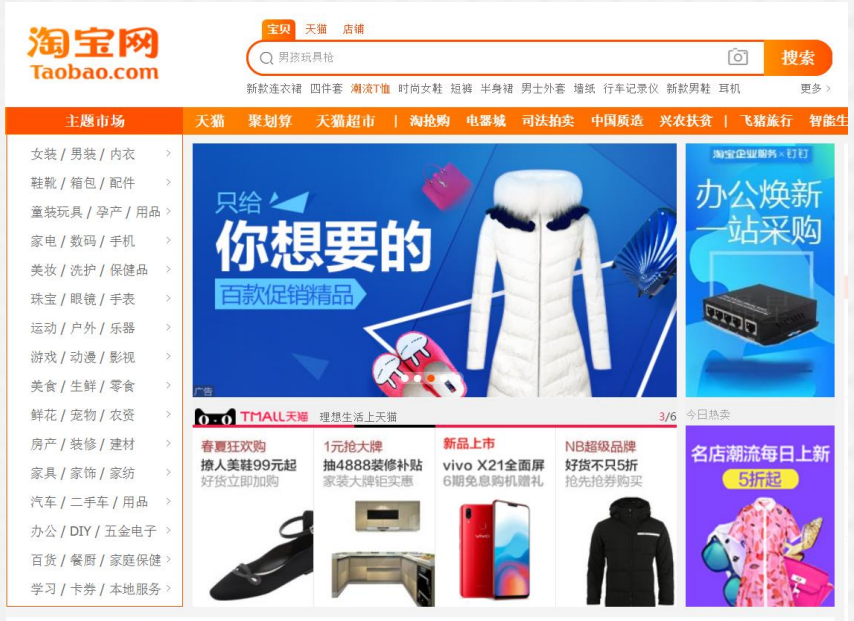
Blockchain Application for User Privacy in Online Transactions

515030910619 汪靖伟

Introduction

Online shopping is an essential component in our life. User privacy in online shopping isn’t protected well.

Online shopping platform, merchant and express company can get user’s id, phone number, preference even real name.



BlockChain

Characteristics

- A distributed ledger.

- Anonymity
- Information cannot be tampered. 51% nodes security
- ……

benefits

- no shopping platform: decentration and economy
- Protect user privacy
- Security

- ……

Method

concepts

Users and merchants are different nodes in this blockchain network. Delivery nodes are also merchant nodes. Intermediary nodes act as an intermediary between user and merchants, not mastered by any instructions
There is no shopping platform but a client for users.

On this client, user can get the goods information from intermediary nodes. Clients also save some personal information and preference natively to provide humanized service.

Method

concepts

Parts of merchant nodes and intermediary nodes are thought as full nodes and preserve all the transaction information, as well some miners in user nodes, to mine new block and get profits. General user nodes are light, and only partly preserve some vital information.

Method

transaction

When user initiates a new transaction to a merchant node, actually user generate a transaction with intermediary node. And intermediary nodes will interact with merchants and express stations.

Method

anonymous delivery

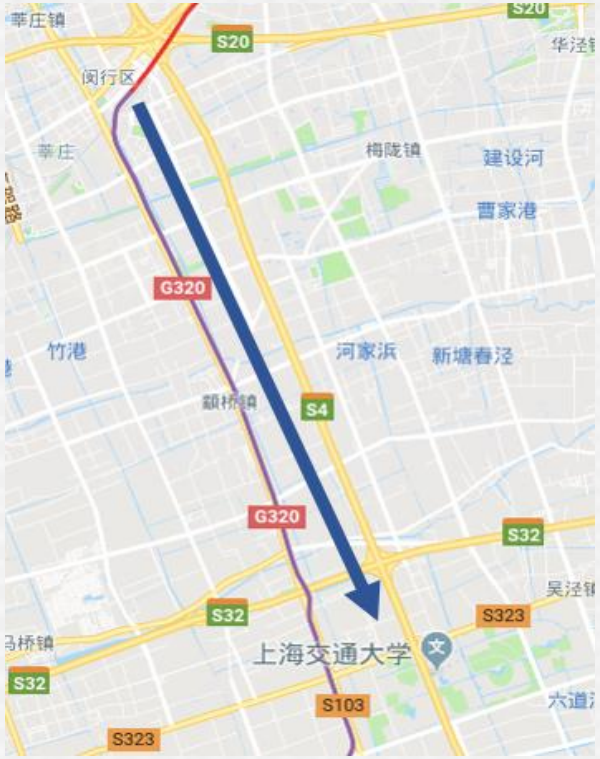
Express nodes are also merchant nodes in this system. They distinct by address. Such as “上海总站”，“上海交通大学站”

User A purchased goods G in Shanghai Jiaotong University where the merchant in Beijing. A’s address will be sent to intermediary node and then be processed as a sequence of express nodes.(specially, “北京总站”，“上海总站”，“上海交通大学站”……)

Method

anonymous delivery

Each delivery nodes would just get the next location from intermediary nodes, and deliver the goods there. For instance, “北京总站” will get “上海总站” but doesn’t know detailed address.



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

```
wjw@wjw-Lenovo-G50-80:~/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: 3082025d02010002818100c8e56b6183ebfc08f96f3f397244377f8fd3c0e34cc3e6007f33c8ffd3bb783f5a05d8137d4ccbbb057715c263e3f9e775c1e5182e4024f76c265f2e851148c8edf16860ee9e57dd55b1bec076d83b33deff851ee
b0b884dacc4163af094261e127c33272431d72f2266021d44413c114a041574e560173d3077d08e6ab3525702030100010281810 0b39cfa8eab05f7c6864cc2383843696331525f68599fe4299990d12a794169572ac382d699f6694802b0dfd176c1c313002
3a5122377d2152caa79fafb99e279bc7f661b27ea5010d413e2cd4e05ff93f208d469983dce24bf95e0c0e0dac3429b253f04d8eddbe67e94afdc056b6cda24913fcab9f4801d5d060063c65c1ce1024100d4e2a5d658418e6fdc83342a01f6878a7ec38f38f
30ce66b29ca53fe88a7dcfbb6d071d3ca09dd5e89fdac09c2a6b75305cd97126a91a1b030c5d8295753a31f024100f1952ce864064c179603af969e75e6d2cbd2b0d49ee99266032da068510c58628bdef3726857ff2db05cbd25ce96b0a76fb47c9a2b30364
2e74d1be84d16e1c9024100a85751ac5dbdf9549b9b64f492f8cfd5c4c7ffc998e8ea8c734f7b7c1bb4221b2a454abd9f568da6e497a42353b961de55086e1e320757446c4d06d22a2c092102407c56de4541ee27cddfed47bb8b157dd73306def2a053f180c
5d3ff0291ec7bb544ee5c789f11e389dd82edeb7e97fa96431d2f209e67f3159e3d06c71a9e535902405fed77578f0aaf6febea3928a78f80538ff7d16c5f043f98ce40937c9c72e1d43ab3bf936b77a0c5e8aa849ea06ff13380107910836 8fc390fbce5091
a584468

Public Key: 30819f300d06092a864886f70d010101050003818d00308189028181 00c8e56b6183ebfc08f96f3f397244377f8fd3c0e34cc3e6007f33c8ffd3bb783f5a05d8137d4ccbbb057715c263e3f9e775c1e5182e4024f76c265f2e851148c8edf168
60ee9e57dd55b1bec076d83b33deff851eeb0b884dacc4163af094261e127c33272431d72f2266021d44413c114a041574e560173d3077d08e6ab352570203010001

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: 3082025c02010002818100daa04ff91cd63159236d485f07f19a79876566463f56a399f9a575d473d1b2cede1c1604f2d1e1f61d54dee0a7c7ea3ea854d8440619d07910806630756e792bf78fbf0aa514d94214b216615af65b0c33387e63
```

Shortcoming

- The shortcomings from bitcoin:
  I. time delay
  II. storage
  III. no real anonymity
- Maybe lose some personalized service

Discussion

- Better anonymity than bitcoin, protect user privacy
- This project based on the first generation blockchain bitcoin, other recent research may have better performance

Thanks