Design of Sharing and Transaction Platform Based on Blockchain

Guohua Xiong[1, a *], Zexin Zhou[2, b] and Jianzhou Zhou[3, c]

[1]GuangDong Construction Polytechnic, GuangZhou 510440, China

[2]GuangDong Construction Polytechnic, GuangZhou 510440, China

[3]GuangDong Construction Polytechnic, GuangZhou 510440, China

[a, *] xiongguohua@gdcvi.net, [b]350679917@qq.com, [c]13288015637@qq.com

[*]corresponding author

Keywords: Blockchain; Ethereum; Sharing and Transaction; Distributed

Abstract: With the development of sharing economy, college students have an urgent need for the transaction management of their idle goods; however, traditional centralized information systems are hard to meet it. By analyzing blockchain technology and taking Ethereum as the basic framework, this paper presents a design of platform, which is decentralized, sharing and transaction, In order to solve the problems existing in the traditional system, such as information leakage, information asymmetry, the data is easy to be tampered, resulting in the transaction can not be traced etc. so lay a solid foundation for platform implementation.

Introduction

With the quick development of internet, E-Commerce, a new commercial pattern, is changingevery aspect of the social economy. Universities, which have always been at the forefront of information technology, are also affected by this business model. Online shopping has become a part of daily life of college students. However, when the purchased goods are not suitable for themselves and cannot be returned, or because of impulse consumption or replacement, the purchased goods become idle goods. The idle goods not only occupy a lot of living space, but also It takes time and energy to organize and maintain, so how to reuse idle resources has become a research hotspot in recent years.

At present, the most famous trading platform for idle goods is Alibaba's "idle fish" platform, but "idle fish" is for the whole social group, and does not provide specialized services for the special environment of campus; some colleges and universities have services to realize idle goods trading, such as WeChat Official Accounts, developing a traditional trading system for second-hand goods etc. , Such systems are often created by third parties and rely on centralized data storage services, which not only has the risk of overall data leakage and information asymmetry, but also occasionally results in arbitrary data tampering, and the credibility of data management is also questioned. Therefore, how to quickly develop a decentralized, secure and reliable Shared trading platform has become an urgent problem to be solved.

1. Key Technologies

1.1 Blockchain. The blockchain technology originated from the foundation paper——《bitcoin: a peer-to-peer electronic cash system》, which is published in the cryptography email group by a scholar under the pseudonym "Sakoshi Nakamoto" in 2008[1]. In essence, blockchain is a set of distributed system. Through consensus mechanism and incentive mechanism, the system is decentralized, safe and reliable. Its core advantage is decentralization. On the basis of implementing point-to-point transaction by using digital encryption technology, the transaction and timestamp can be written into a block based on proof of work (POW), and then the block can be added to an

unlimited chain structure, and the whole network is encouraged to maintain the correct extension of the chain by incentive mechanism [2] [3][4][5].

Although blockchain technology has solved two important problems in the field of digital cryptocurrency for bitcoin system for a long time, i.e. double spending problem and Byzantine general's problem [6], as a new technology, when using blockchain technology for the application scenarios outside the field of digital cryptocurrency, there are still many challenges, how to design a reasonable intelligent contract that plays a decisive role in transaction parallel verification should bear the brunt.

1.2 Ethereum. In December 2013, vitalik buterin proposed the Ethereum blockchain platform [7], which is the representative product of the second stage of blockchain development. On this platform, the blockchain system was fist enabled to implement Turing, which makes it possible to develop and use applications in the blockchain system, and can guarantee the effective execution of the program. As a typical representative of blockchain Technology 2.0, Ethereum has the following advantages:

(1) Support intelligent contracts. The languages used to develop Ethereum intelligent contracts are Serpent, Solidity, Mutan, and LLL etc. Among them, Solidity supports inheritance and polymorphism, and provides direct access to the global variables that have parameters related to the blockchain nodes. Blockchain, at the same time, Solidity has all the built-in features of the Serpent language, its' syntax rules are similar to JavaScript and easy to learn, so it is officially recommended for use.

(2) Faster Transaction Speed. Adopt new consensus algorithms (such as POS, DPOS, etc.). By dividing intelligent contracts into different logical areas, intelligent contracts in each area are executed sequentially, and throughput can be increased between different areas in parallel. , So it can meet the demand for transaction speed in most application scenarios.

(3) Support Information Encryption. Through advanced cryptographic technologies such as Zero-Knowledge Proof, ring signature, and Homomorphic Encryption, the information that needs to be sent and received is encrypted to protect the privacy of both parties in the transaction.

(4) Zero Consumption. With the emergence and application of new consensus algorithm, each node in the blockchain no longer needs to reach a consensus through consuming computing power, that is, achieving zero consumption of resources, so it can be green deployed.

2. Design of Sharing and Transaction Platform

The system generally adopts a distributed architecture based on Ethereum. The top layer is the application layer, which mainly displays some relevant interfaces with user operations, such as system management, transaction management, credit management, track and trace management modules etc.; The intelligent contract layer includes virtual machine that executes scripting language and distributed application development, it presents the complete combination of intelligent contract and the front end interaction interface to services for users. The consensus layer uses a consensus mechanism based on proof-of-work to allow a system with decentralized decision-making power to reach an agreement; in the incentive layer, each node can solves a mathematical problem through competition in computing power, and rewards the first node to solve the problem, so as to promote the whole network to achieve computing power competition; The network layer is a distributed network, which mainly implements mutual communication between Ethereum nodes through P2P networks [8] [9], message propagation mechanism and data verification; The data layer encapsulates the block's data structure and data encryption related content; the storage layer mainly uses the interstellar file system to implement data storage of the entire system, as shown in Fig 1.

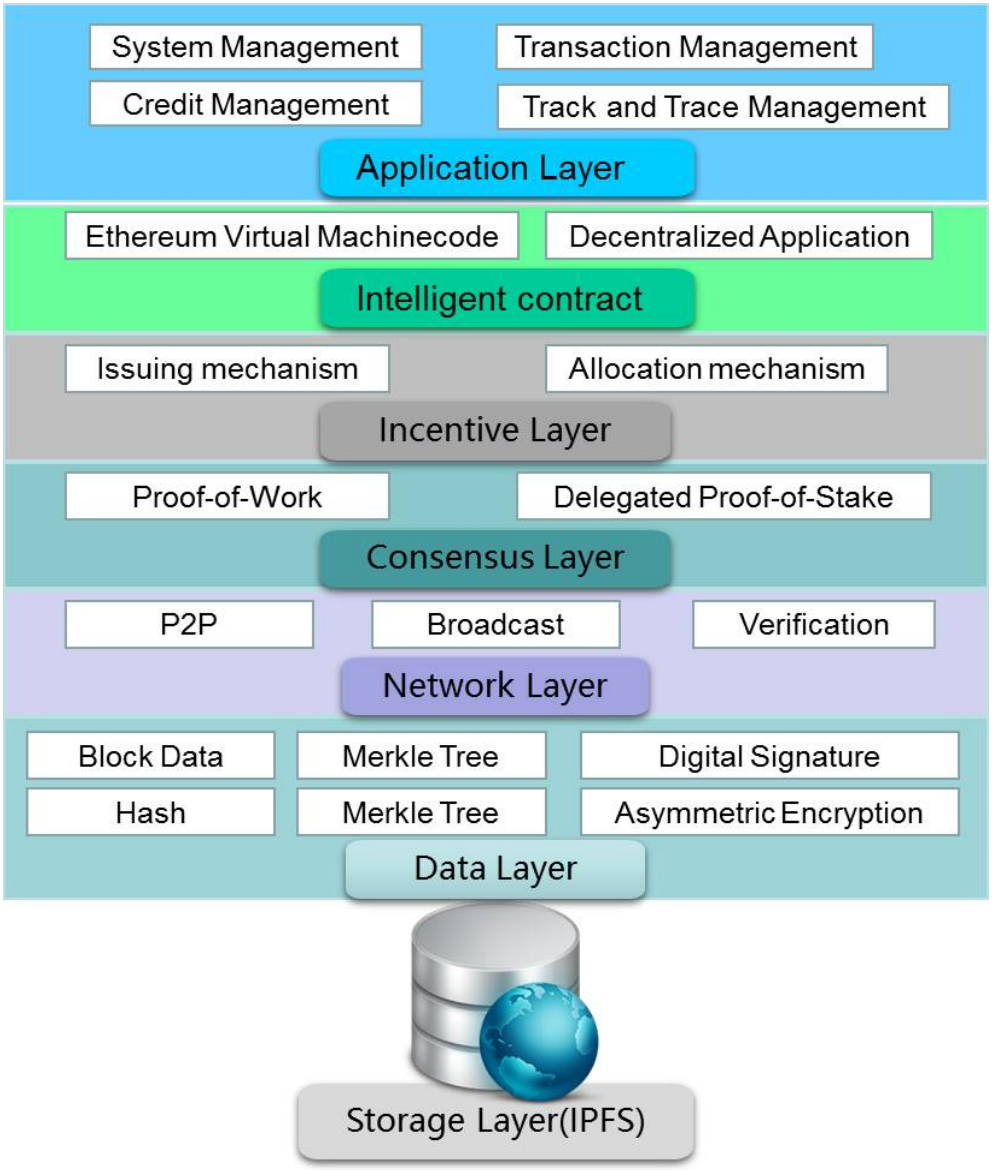

Figure 1. Sharing and transaction platform system architecture

3. Summary

Based on the analysis of blockchain technology and Ethereum architecture, a architecture design of sharing and transaction platform is proposed. Which solves the problems of traditional second-hand trading system, such as information leakage, information asymmetry, data easy to be tampered, resulting in the transaction can not be traced etc.. However, there are many aspects in this solution that need to be improved, for example the design of intelligent contracts, which need to be improved in the later stage.

References

[1] Nakamoto, S.Bitcoin: A peer-to-peer electronic cash system, Information on https://bitcoin.org/bitcoin.pdf, (2019).

[2] Becker J., Breuker D. and Heide T.et al. Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In: Böhme R. (eds) The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg, (2013), pp: 135-156.

[3] Wright, Aaron, and P. De Filippi. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Electronic Publishing*, (2015).

[4] Ametrano, Ferdinando M. Bitcoin, Blockchain, and Distributed Ledger Technology. *Social Science Electronic Publishing* (2016).

[5] Dennis, Richard. Rep on the block: A next generation reputation system based on the blockchain. *Internet Technology & Secured Transactions* IEEE, (2016).

[6] Andreas M. Antonopoulos: *Mastering Bitcoin: Unlocking digital crypto-currencies*(O'Reilly Media, USA 2014).

[7] NButerin V.A next-generation smart contract and decentralized application platform, GitHub: ethereum/wiki, 2014.https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Pager,2014

[8] Stoica, Ion, et al. Chord: A scalable peer-to-peer lookup service for internet applications. *ACM SIGCOMM Computer Communication Review* 31(2001).

[9] Herbert, Jeff, and A. Litchfield. A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology. P*roceedings of the 38th Australasian Computer Science Conference (ACSC 2015)*2015.