Proceedings of the 8th International Conference on Economic Management and Green Development
DOI: 10.54254/2754-1169/119/20242355

Transforming the Game Account Trading Market: An Ethereum Blockchain-Based Solution

Qianshuo Yu[1,a,*]

[1]*FIE, Macao University of science and technology, Macao, China*
a. 1210027225@must.student.edu.mo
**corresponding author*

Abstract: The primary risks associated with game account trading include the exposure of personal information and the potential for account retrieval. In a system leveraging blockchain technology, specifically Ethereum combined with the InterPlanetary File System (IPFS), personal and game-related information is kept confidential. This system ensures that only the respective users have access to their personal data on the blockchain. Furthermore, upon the completion of a trade, the information associated with the account can be altered once, enhancing security. Additionally, the landscape of video game trading, particularly in China, is evolving rapidly. With the growth and development of the video game industry in the region, it has become increasingly challenging to trade game accounts. This complexity is largely due to the emergence of various policies and regulations that aim to safeguard user data and maintain the integrity of game ecosystems. The blockchain-based system provides a more secure and efficient way of handling these transactions, mitigating risks associated with traditional trading methods. By employing decentralized technologies, this innovative approach ensures greater privacy, security, and compliance with regulatory standards, thus revolutionizing the realm of game account trading.

Keywords: Revolutionizing, Game, Account, Trading, Blockchain

1. Introduction

Since Satoshi Nakamoto proposed a point-to-point electronic cash system leveraging cryptography and distributed ledger technology, Bitcoin has gained increasing popularity and diverse applications [1]. This technology, rooted in the innovative concept of blockchain, has certain limitations, including the slow speed of transaction processing.

Ethereum, developed by Vitalik Buterin, is another decentralized cryptocurrency. It facilitates the easy deployment of smart contracts, allowing developers to use the Solidity language in an Integrated Development Environment (IDE) for creating these contracts [2]. Ethereum can also be integrated with MetaMask for executing various commands. While blockchain technology ensures that stored information is permanent, immutable, and traceable, it faces limitations in data capacity. For instance, Bitcoin's blockchain can only accommodate 1MB of information per block [3]. Ethereum's blockchain allows for greater data storage, but this comes with increased costs.

The Interplanetary File System is a peer-to-peer distributed file system without a centralized server [4]. It is capable of storing larger amounts of data for blockchain applications. IPFS generates a unique and verifiable Content Identifier (CID) based on file content, acting as both a hyperlink and proof of

DOI: 10.54254/2754-1169/119/20242355

the file's content. Consequently, recipients can access and authenticate files using the CID. Importantly, the CID's size (a 256-bit string) is comparatively small and can be efficiently distributed within the blockchain for data integrity verification and access [5].

The trading of game accounts has become a contentious issue. Experienced players often wish to sell accounts they no longer use, and newcomers seek to buy these accounts from seasoned players, benefiting both parties. However, in China, the framework for game account trading is not conducive [6]. One major issue is the tight coupling of game accounts with personal information, creating a risk of private data being compromised during transactions [7]. Furthermore, many video game companies have policies allowing players to retrieve accounts using identity card information, leading to a secondary problem where sellers can reclaim and resell their accounts multiple times.

2. Relevant Theories

2.1. Definition and principles of blockchain technology

The fundamental technology of numerous cryptocurrencies is blockchain. Blockchain has drawn a lot of research interest as a distributed ledger system. Unlike traditional databases that are controlled by central authorities, blockchains are decentralized and managed by a peer-to-peer network. This indicates that no one party controls the entire chain and that the network is maintained by all parties working together [8].

Every transaction on a blockchain is accessible to everybody with network access. Transparency and trust are increased when each participant may review the transaction history. A transaction cannot be changed or removed from the blockchain once it has been recorded there. The immutable record-keeping is a crucial component of blockchain's security and reliability.

2.2. Smart Contract

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network [9]. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

Because the conditions of the agreement and the contract's execution are well specified and documented on the blockchain, smart contracts facilitate the trade of gaming accounts with a higher level of confidence and transparency. This lowers the possibility of fraud or deception and does away with the necessity for middlemen. Since they are made to be tamper-proof and can help guard against fraud and misrepresentation, it can also offer further security for transactions using used game accounts.

However, the effect of vulnerabilities in smart contracts increases with the complexity of smart contracts and the diversity of application scenarios [10]. Attacks against smart contracts are common because they store large amounts of money and are immutable once they are posted to the blockchain. When malicious actors target smart contracts, the implications are frequently more severe than when they target conventional network systems.

2.3. IPFS

Blockchain applications interact directly with blockchains or smart contracts to reach a consistence on the contract, code and function. This can lead to the following problems when dealing with large data files. These files are usually unessary for the operation of blockchain, it will becomes bloated which lead to the data being copied on a large of number.

DOI: 10.54254/2754-1169/119/20242355

It is inefficient for blockchain to store document which take up a lot of memory. Because of the limitation of memory, the document outside the blockchain must be spliced and restructured again which also require additional data about the restructured document. This means that more memory is needed to keep these information. It is valuable for smart contract to store the file directly so that users can easier to check information in blockchain. Nonetheless, it costs a lot for smart contract to send and store large memory file even though part of them.

According to the above information, blockchain is not a proper place to send and keep large memory file. However, developer can use file sharing platforms to run applications meanwhile in a tiny space so that users can send large document easily. A cryptographic hash value can be sent to the blockchain and used at security identification. This job will be taken by Interplanetary File System (IPFS) technology. It can use the hash value to verify and transmit.

2.4. Game Trading Background

According to the interim measures for online games published by China government, all the players must render their personal information such as their real name and identify id to play the video games. This policy aims to protect the minors away from video games but at the same time lead to many challenges for the business of game account.

In the past, the trade of game account only requires the username and password which are bounded to smart phone or e-mail. Once the buyer pays money, seller will send the username name and password to the buyer and ask the buyer to switch the bounded phone or e-mail. But now the personal information is also bounded with the game account and cannot be changed. If the account is sold, its owner's personal information has the risk to be usurped by the buyer.

In order to help users find their lost account back, many video company publish a function that players can use their identify id to retrieve their account.

This means that seller can get back his account even though he has been sold his account.

3. System Analysis and Application Research

Figure 1. shows the whole procedure of this trade. In the whole system, the seller and the buyer reach an agreement through consultation and decide to trade the game account. Then log in at the front end and verify the identity of the buyer, and then connect metamask. Metamask is a virtual wallet system, which can connect with the money spent by Ethereum and jump to smart contracts to realize various functions. Metamask then wakes up the smart contract to modify the personal information and account information of the seller's original account. In this process, the buyer can only modify the original seller's information, so as to ensure that the seller's personal information will not be exposed. Finally, when the transaction is completed, the seller receives the transaction completion information from the front end, and the game account is completely transferred from the seller to the buyer.

DOI: 10.54254/2754-1169/119/20242355

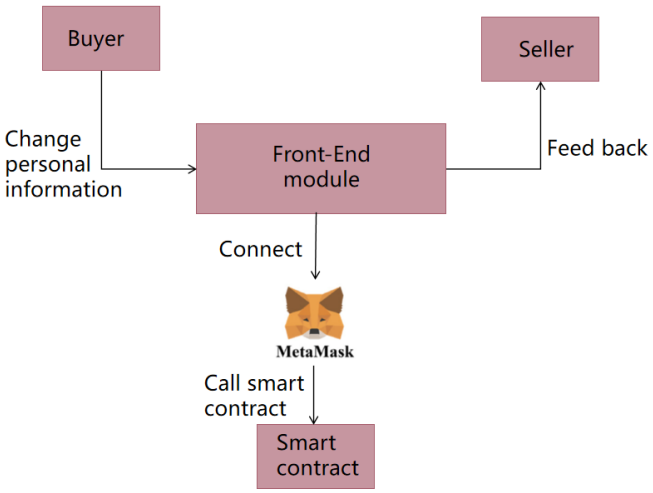

Figure 1: Procedure of game account trade (Photo/Picture credit: Original).

3.1. Frontend: Design and functionality of the user interface.

The front-end module uses ReactJS to create user interfaces, which can reduce development and maintenance time by employing reusable components. With the help of web3.js, Ethereum blockchain interaction is supported, enabling DApp developers to submit queries to the blockchain's smart contracts to add or retrieve data by connecting to the network's nodes via HTTP, JSON, and WebSocket. To access and utilize the DApp services, a browser is required.

3.2. Contract Partition

The verifier utilize the verify contract to finish the system's verify process, enabling access to and modification of the private information bound by the account as well as the account information stored in the blockchain. In this manner, the system contains all of an account's records. When the seller plans to sell the account, he can use the account contract's user name to look for account information. After filling out the account status, he can use the commodity contract to upload the automobile sales data to the system. Through the order contract, prospective purchasers can finalize the deal. Users can download the account history report if they have already registered pertinent account records in the system. Account transfer data, account equipment information, and role ability information are all included in each historical report. The buyer can use the system to request that the seller of the used account download the historical report in the event that the seller refuses to deliver it. Through the license agreement, the seller has the option to approve or deny the request. The buyer can get the account's historical report from the system as soon as the seller approves the request. Additionally, the license contract gives the vendor the ability to revoke this license at any moment.

3.2.1. Verify contract

The verifier's job is to assist the buyer and seller in the transaction process. Firstly, the verifier enters the system through the authentication contract and sends his private address of Ethereum to the system so that the system can identify him as the verifier instead of the seller or buyer in the future. Then the verifier sends the electronic contract to the system and stores it in IPFS. The electronic contract will be encrypted layer by layer. IPFS will return a unique hash value to the system and store it in the blockchain by smart contracts. The system can access the encrypted contract and password with this hash value, but it needs to decrypt the password with the private key before accessing the contract

DOI: 10.54254/2754-1169/119/20242355

with the password. If the contract is correct, the system will ask the verifier to pay a certain amount of Ethereum to complete the whole verification process.

3.2.2. Account Contract

After completing the authentication, the verifier will assist the interested seller to register the game account. The seller will provide the verifier with the transaction record, equipment, role and property status of the account. Then the verifier will send a registration request to the system according to a unique account id. After the request is passed, the information will be stored in IPFS, waiting for the buyer to make a transaction.

3.2.3. Commodity Contract

The commodity contract includes two parts: the buyer's inquiry and the seller's uploading data, which must be operated by the seller himself, otherwise the transaction will be rejected. First, the buyer inquires about the corresponding vehicle in the contract through the unique id of the vehicle. You can also enter user preferences such as rank, combat ability, specific roles, etc. This information will be converted into JSON format and then passed to IPFS. On the other hand, the seller can choose to transmit the account information to the commodity contract after passing the account contract. The account details will be transmitted to IPFS, and the hash value returned by IPFS will be returned in the commodity contract. If the uploader's ethereum address is different from the seller's ethereum address in the account contract, the transaction will be interrupted. Any non-seller and buyer can inquire about commodity information through commodity contracts, such as account numbers and transaction records.

3.2.4. Trading Contract

The trading contract mainly realizes the specific process of buying and selling. If the buyer decides to buy the seller's goods, he can send his own quotation to the seller. This offer may be lower than the seller's expected price or equal to. If both the buyer and the seller agree on the price, the buyer can log in to the game account to verify the virtual property such as props and characters in the game, and the personal information bound to the account still belongs to the seller. After the buyer and seller confirm the transaction, the verifier will help the buyer exchange his personal information with the seller information stored in the blockchain through the front end to realize the complete transfer of the account to the buyer. Finally, the system will ask the buyer and seller to confirm the order to realize the whole transaction process.

3.2.5. After-sale contract

This contract mainly solves the situation that the buyer's account number is still found after the transaction. Although this system encrypts the contract and stores the account information in the blockchain, it still cannot completely prevent the account from being retrieved. Therefore, after the account is retrieved, the buyer traces back to the traded account order through the buyer's own Ethereum address, and requests the verifier to check the account information stored in IPFS. The verifier will modify the real name information, telephone number, email and other information of the account again. If you still can't get your account back, you can pursue the responsibility through the personal information provided by the seller before.

DOI: 10.54254/2754-1169/119/20242355

3.3. Gas assessment

"Gas" is the unit of measurement used in the context of smart contracts, specifically on the Ethereum blockchain, to indicate the amount of computing work needed to carry out tasks like transactions and smart contract interactions. Computational resources are needed for every Ethereum network operation. Gas is the price paid to network validators—miners in a Proof of Work scenario or validators in a Proof of Stake scenario—for processing and validating transactions. Gas is used on the Ethereum blockchain to distribute resources and prevent spam from entering the network. It guarantees that resources are used effectively and that the network is not overburdened with pointless or too complex activities by charging for each computation that is performed on it. The cost of this system is obtained by the following two formulas (1), (2).

$$GweiPrice=Ether/10^9 \quad (1)$$

$$USDCost=GweiPrice*GasCost \quad (2)$$

4. Challenges

The main challenge of the account trading system is whether the government supports the trading of account numbers. Due to policy restrictions, it is difficult to change personal information, especially identity information, in game accounts. This leads to the complicated transaction steps and can't make full use of the advantages of blockchain to solve various problems. Secondly, there is still a double verification process of mobile phone verification code and email verification code under the verification of personal information. Although this process can be realized relatively easily when trading accounts, it is still difficult to be stored in the blockchain. Further more, the convenience of game account trading will affect the government's management of the game. For example, through this system, teenagers can easily buy game accounts and skip the government's restrictions on minors playing games. For this, users may see the contract of minor authentication information in the system in the future. Finally, the situation of verifiers also arise crisis of confidence. Because of the particularity of the verifier's identity, he can see all the information of the buyer and the seller, which means that new identity information leakage may occur. So this position needs very trustworthy people, especially government officials, which means that the whole system needs government support.

5. Conclusion

In summary, this system primarily stores game account information within the blockchain, safeguarding private information through multi-layered encryption. It encompasses various contracts: verification, account, commodity, trading, and after-sales. These contracts collaboratively ensure the fairness and integrity of account transactions. The role of the verifier is pivotal in this ecosystem, facilitating transactions by overseeing sellers and managing account information updates. However, a key concern arises: the ability of the verifier to protect the privacy of both buyers and sellers. This intricate system operates by encoding game account details on the blockchain, a method that not only secures sensitive data but also streamlines the transaction process. Each type of contract plays a unique role; the verification contract validates participant identities, the account contract manages user credentials, the commodity contract oversees the listing of accounts for sale, the trading contract handles the transaction mechanics, and the after-sales contract addresses any post-sale issues. The verifier, acting as an impartial entity, ensures compliance and fairness, thus enhancing trust among participants. Despite these mechanisms, the effectiveness of the verifier in maintaining the confidentiality of the parties involved remains a pressing concern. This aspect is crucial, as it directly

DOI: 10.54254/2754-1169/119/20242355

impacts user trust and the system's overall credibility. Ensuring robust privacy protection within this framework is essential for its long-term success and user acceptance.

References

[1] *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.*

[2] *Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.*

[3] *Steichen, M., Fiz, B., Norvill, R., Shbair, W., & State, R. (2018, July). Blockchain-based, decentralized access control for IPFS. In 2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData) (pp. 1499-1506). IEEE.*

[4] *Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. ICT express, 6(2), 93-97.*

[5] *Li, P., Wang, G., Xing, X., Zhu, J., Gu, W., & Zhai, G. (2024). Detecting abnormal behaviors in smart contracts using opcode sequences. Computer Communications.*

[6] *Blum, A. (2019). Blockchain and trade finance: A smart contract-based solution. University of Basel.*

[7] *Su, Y. J., Chen, C. H., Chen, T. Y., & Yeah, C. W. (2023). Applying Ethereum blockchain and IPFS to construct a multi-party used-car trading and management system. ICT Express.*

[8] *Zhu, X., Xu, H., Zhao, Z., & others. (2021). An Environmental Intrusion Detection Technology Based on WiFi. Wireless Personal Communications, 119(2), 1425-1436.*

[9] *Scholten, O. J., Hughes, N. G. J., Deterding, S., Drachen, A., Walker, J. A., & Zendle, D. (2019, October). Ethereum crypto-games: Mechanics, prevalence, and gambling similarities. In Proceedings of the annual symposium on computer-human interaction in play (pp. 379-389).*

[10] *Berentsen, A. (2019). Aleksander berentsen recommends "bitcoin: a peer-to-peer electronic cash system" by Satoshi Nakamoto. 21st Century economics: Economic ideas you should read and remember, 7-8.*