DESIGN AND IMPLEMEMTATION OF BLOCKCHAIN-BASED DIGITAL COLLECTION TRADING PLATFORM

Li Sun[1], ZhiGang Han[2] and Zhulei Huang[2]

[1]Department of Electrical and Computer Engineering, Chengxian College, Southeast University, NanJing, JiangSu, CHN
[2]College of Computer and Information Engineering ,Nanjing Tech University, NanJing, JiangSu, CHN

ABSTRACT

A blockchain-based digital collection trading platform has been developed, with a front-end design rooted in the Vue.js framework and Element UI component library. This front-end implementation encompasses various functionalities such as a search box, navigation bar, collection list, detail page, and transaction process. On the other hand, the back-end is constructed using the Springboot framework, mysql database, and kafka, integrated with a custom-built blockchain system operating on the Linux platform.

In the design of this blockchain system, the traditional "mining" function, which competes for the right to create blocks, has been eliminated. Instead, the main server assumes the responsibility of block creation. Leveraging the characteristics of the Merkel tree and the Merkel Patricia tree, the platform explores the application of a coalition chain that aligns more closely with the concept of centralisation.

Furthermore, this platform places significant emphasis on the security design of the transaction system, ensuring robust and secure transactions within the digital collection trading environment.

KEYWORDS

blockchain technology, federation chain, SpringBoot framework, digital collections

1. INTRODUCTION

With the continuous updating of blockchain technology and the rise of meta-universe, the digital collectibles industry has been developing rapidly worldwide, attracting a large number of enterprises and capital. Digital collectibles represent the epitome of the digital economy and the meta-universe, referring to digitally created cultural and artistic items that are distinctly identified through blockchain technology. These encompass various forms such as paintings, illustrations, audio clips, videos, 3D models, and more. Digital collections are able to protect their digital copyrights and enable digital distribution, purchase, collection and use.

Blockchain technology has been updated in three versions. The initial phase, referred to as the programmable currency stage, facilitates direct payments between individuals who lack mutual trust through the use of Bitcoin, thereby enabling the seamless circulation of virtual currencies across the internet; the second stage is known as the programmable finance stage, in which

David C. Wyld et al. (Eds): SE, SAIM, SIPM, CoNeCo, ICITE, ACSIT, CMIT, FCST, SNLP – 2024
pp. 11-09, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.140802

people are beginning to apply blockchain to other financial fields such as stocks, clearing, private equity, etc., such as the R3 Consortium; and the third stage is the programmable society stage, in which people are applying blockchain to a variety of in-demand areas, such as anonymous voting, supply chain, IoT, smart healthcare, smart cities, 5G and AI, etc. NFT technology can initially be traced back to 2012, when an improved peer-to-peer network protocol based on Bitcoin enabled decentralised digital asset transactions, and projects such as Counterparty and CryptoKitties have since sprung up to make NFT the mainstream. In China, due to the implementation of policies related to virtual currencies, blockchain is mainly used in the financial sector, while the promotion of NFT-based digital item transactions is hindered by the risks of property rights, value and technology. However, domestic Internet giants such as Ant, Tencent and Baidu have begun to explore the application prospects of NFT, so NFT technology will become an important infrastructure of the meta-universe.

2. OVERALL SYSTSM DESIGN PROGRAMME

The front-end design of the platform is based on the Vue.js framework and the Element UI component library, which implements the functions of search box, navigation bar, collection list, detail page and transaction process. In the implementation, we used front-end technologies such as JavaScript and CSS, and used blockchain technology to ensure the uniqueness of digital collections and the security of transactions. Finally, by interacting with the back-end API, we realised the functions of uploading, displaying, searching and trading of digital collections, which provides a new way for the trading of digital collections.

The overall architecture of the blockchain-based digital collection trading platform is shown in Figure 1, where users operate on the front-end web page. Among them, the operation request about user information and digital collection information is passed to the back-end, and the back-end operates on the database according to the request; the operation request about the transaction amount is passed to the back-end, and the back-end reads or creates a new block operation on the blockchain according to the request.

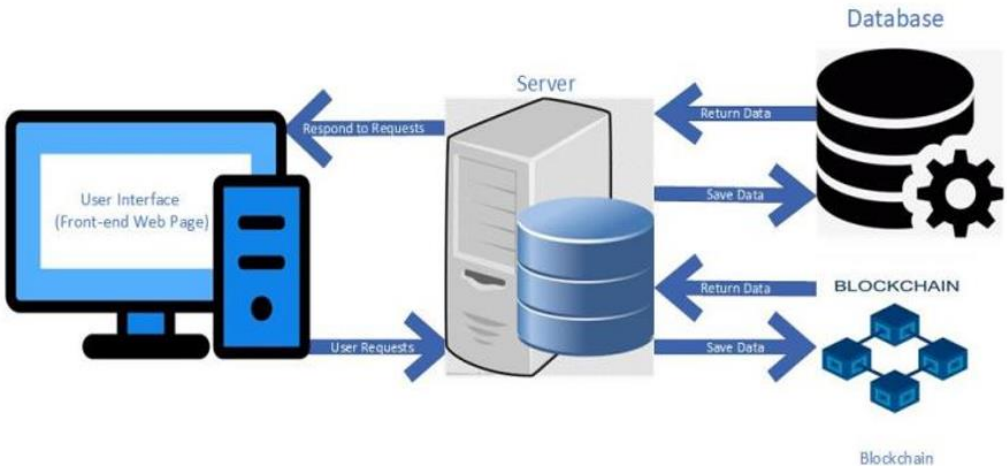

Figure 1 General architecture of the trading platform

This system is generally divided into three major sub-systems, and the functional structure is shown in Figure 2. The digital collection system is responsible for digital collection-related functions, the user system is responsible for user-related part of the functions, and the blockchain system is responsible for storing transaction information and user balance. Users can conveniently complete the functions of uploading, trading, managing and order enquiries of new

products through this platform. The platform uses the distributed Springboot framework as the backend, uses kafka to pass information between various servers, and uses Vue.js technology to write the front-end page. At the same time, it uses a storage model combining mysql database to save user and digital collection information and blockchain to save transaction information.

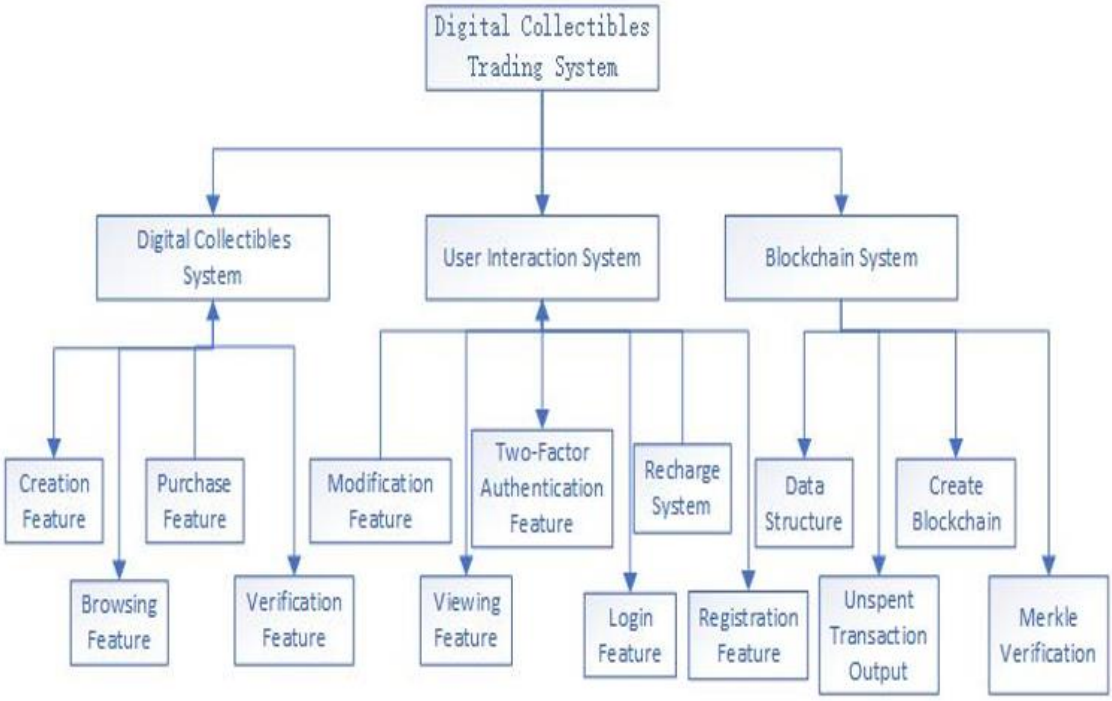

Figure 2 System Functional Structure Diagram

3. TRADING SYSTEM SECURITY DESIGN

The security of digital transactions is crucial, especially in today's digital age, which involves the transfer and exchange of value. Lack of security can lead to theft, fraud and data breaches, causing serious losses to individuals and organisations. Securing personal and financial information has emerged as a crucial task as an increasing number of individuals adopt digital currencies and online payment systems for their transactions. Emphasising the security of digital transactions can therefore protect the interests of participants, increase trust and contribute to the development of the digital economy.

The design ensures secure transactions throughout the process by storing data in multiple nodes in a distributed manner, thereby guaranteeing the security and reliability of the information. Each transaction is encrypted and verified and once confirmed, it is added to the tamper-proof blockchain. This mechanism makes the blockchain highly secure and trustworthy for digital transactions. A detailed statement of the system transaction security scheme is given below.

3.1. Transaction Security

Storing transaction information related to collections among users in a database is inappropriate. Through this information, we can discern the previous and current owners of collections, as well as the time of the transactions, thereby determining whether a user legally possesses the collection. However, even when these data are encrypted within the database, there remains a risk. If others were to discover the encryption rules and subsequently manipulate the transaction

details of numerous blocks, we would be unable to accurately ascertain the ownership of the collections. Legitimacy and compliance of the collection, so the transaction information of the collection is put into the chain and encrypted, which makes it difficult for the invaders to modify or unable to modify a large number of blocks at a low cost, and such a design guarantees the truthfulness and validity of the information of the collection, and also protects the user's property.

3.2. Conversation Security

HTTP is a stateless protocol, meaning that it lacks the capability to keep track of the status of a connection. The absence of state means that the server cannot confirm whether this request and the next request originate from the same client. However, according to our common sense, if a user logs in successfully, the next request should be bound to that user. For example, if you add a shopping cart, each time you add a product, it should be added to the corresponding user's shopping cart, so the server must identify the user, which is actually a function of user authentication.

To do this, we first front-end send our username and password to the back-end interface via a web form. This process is typically an HTTP POST request. The recommended way to do this is through SSL encrypted transmission (https protocol), thus avoiding the sniffing of sensitive information. After the back-end checks the username and password successfully, the user's id and other user information as a JWT Payload (load), and the header of the Base64 encoding and splicing respectively after the signature, forming a JWT (token). The JWT is a string of the form lll.zzzz.xxx. token:head.payload.signature The back-end will return the JWT string to the front-end as a result of a successful login, and the front-end can save the result in localStorage or sessionStorage, and then delete the saved JWT when it exits the login. When logging out, the front-end can delete the saved JWT. Front-end will put the JWT into the Authorisation bit of HTTP Header in each request. (To solve XSS and XSRF problems) The backend checks if it exists, and if it exists, verifies the validity of the JWT. For instance, you may need to verify the correctness of the signature, determine if the Token has expired, and optionally, confirm that the recipient of the Token is indeed yourself. After the validation passes, the back-end uses the user information contained in the JWT to perform other logical operations and return the corresponding results.

3.3. Blockchain Technology

Blockchain technology was initially conceived as a decentralised ledger system specifically tailored for Bitcoin, empowering users to execute transactions sans the requirement of any intermediary. The core mechanism of blockchain is the use of cryptography to encrypt a block of data into a "block" and link each "block" in turn to form a tamper-proof "chain". chain". The advantage of this technology is that it ensures the security and transparency of transactions. All participants on the network can view all transaction records, and all transaction records are stored simultaneously on each node, so they cannot be tampered with by a single participant. In addition, blockchain technology reduces the cost of transactions as well as increasing their efficiency as there is no centralised institution involved.

In designing the blockchain system, the "mining" function of competing for the right to create blocks was eliminated in favour of creating blocks for the master server, and the characteristics of the Merkel and Merkel Patricia trees were adopted to explore the application of a more centralised idea of federated chains.

3.3.1. Block Composition

Figure 3 depicts a block within a blockchain. In blockchain technology, each block consists of some specific attributes. These attributes include:

(1) Block number: the number of this block, the genesis block is number 0, after that, every time a new block is created, the block number will be added one in turn.
(2) Timestamp: the time when the block was created. This is an important property because it ensures that each block is independent in time.
(3) Number of transactions: the number of transaction messages recorded in the Merkle tree. This attribute tells us how many transactions were processed in this block.
(4) Previous Block Hash: The hash value of the previous block is recorded as a crucial piece of information, serving as a means to verify that the previous block has remained unaltered.This attribute is very important as it ensures the integrity and correctness of each block in the blockchain.
(5) This block hash: a hash of all information within the block header of this block. This attribute, derived from all attributes present in the block header, serves to uphold the integrity and accuracy of the block.
(6) Transaction Tree Root: A transaction tree is a Merkel tree that holds all transaction information within it. This attribute is a key technology in blockchain technology that enables the composition of multiple transaction messages into a transaction tree and provides integrity guarantees for these transaction messages.
(7) Status Tree Root: The status tree is a Merkle Patricia Tree that holds balance information for all users.

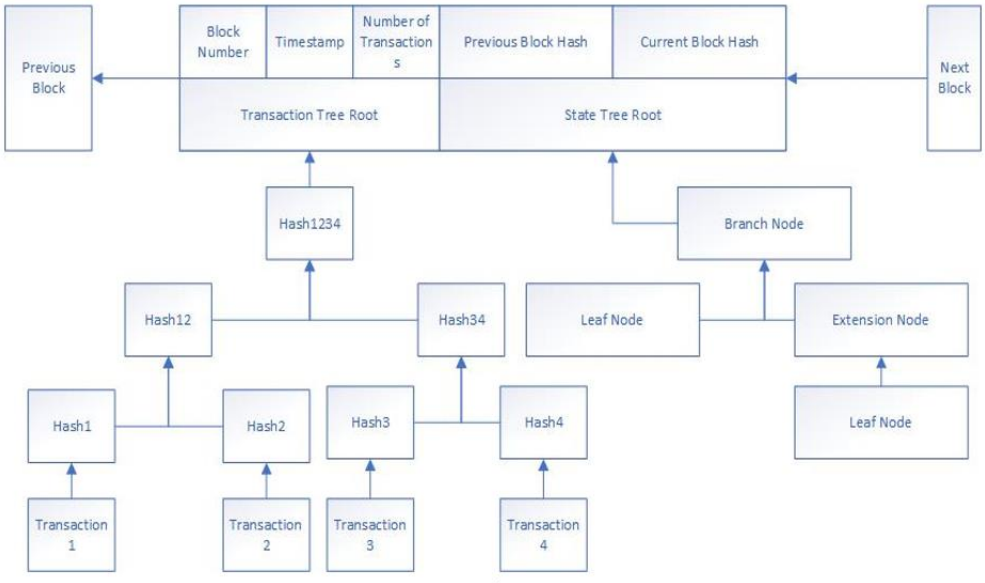

Figure 3 A block in the blockchain

3.3.2. Merkel Validation

To determine if a transaction, such as a yellow-coloured one, has been recorded in a blockchain depicted in Figure 4, a light node can inquire with a full node for the red-coloured hash values. Using the known transaction content and the red-coloured hash pointers, the light node can then progressively calculate the green-coloured hash values to derive the Merkle root. This calculated

Merkle root is subsequently compared with the Merkle root stored in the block header. If the two roots match, the verification is successful, indicating that the transaction has indeed been recorded in the blockchain. However, if they differ, the verification fails, signifying that the transaction has not been properly recorded.

The block creation function uses a timed task for blockchain transactions. It first gets all pending transactions from the transaction list and then processes each transaction separately. If the transaction is made by the root node of the system, it will directly set the transaction status to 1 and store it in UTXO (unused transaction output), and at the same time store the transaction record in the database; otherwise, it needs to judge whether the balance of the buyer's account is sufficient or not, as well as whether the relevant information is consistent with that of the UTXO and the status tree, and if the judgement is successful, then it will set the transaction status to 1 and store it in the UTXO and the status tree; if it is unsuccessful, then it will set the transaction status to 2 and store it in the database. If it fails, the transaction status will be set to 2 and stored in the database.

Subsequently, the block header is created and populated with the values of its various attributes. This process involves various components such as the block's index within the blockchain, the timestamp, the count of transactions contained, and the information regarding the previous block. Furthermore, it generates the root hash of the current block, the state tree hash, and the hash of the block itself, all through the utilization of the Merkle tree.Finally, the list of pending transactions is emptied to complete this block creation operation.

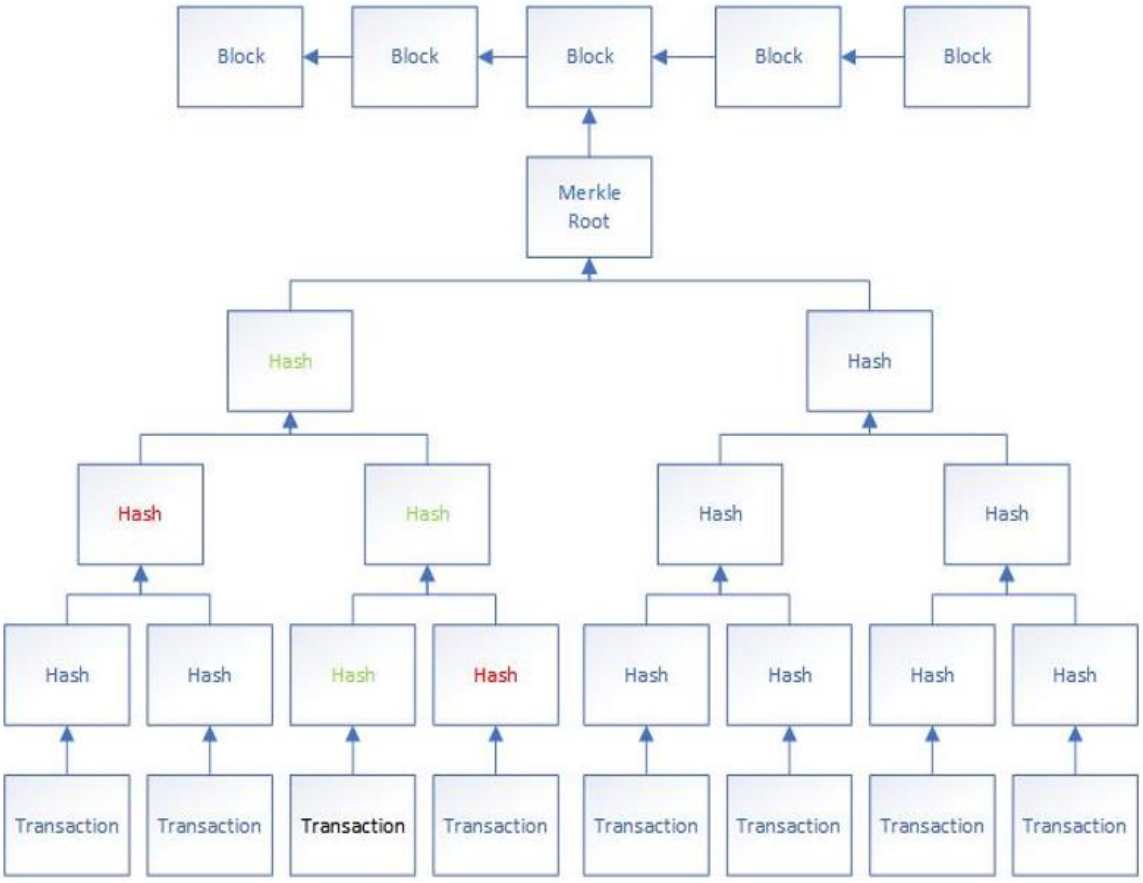

Figure 4 A blockchain

4. CONCLUSIONS

The blockchain-based digital collectibles trading platform addresses the challenges faced by the traditional digital art market by securely storing transaction information on the blockchain. Leveraging the blockchain's inherent non-tamperable and traceable characteristics, the platform ensures the safety, transparency, convenience, and efficiency of digital collectibles trading for its users.

By integrating various technological advancements and adopting key technologies such as blockchain and encryption algorithms, the system facilitates a more intelligent, standardized, and sustainable transaction process. This comprehensive approach enables functionalities like casting, offering, trading, collecting, and tracing of digital collectibles, providing a comprehensive solution for the digital collectibles market.

ACKNOWLEDGEMENTS

With the completion of this blockchain-based digital collection trading platform project, I express my deepest gratitude to my mentors, peers, and loved ones. Your support, suggestions, and encouragement have been pivotal in my journey. Thank you for being there.

REFERENCES

[1] Qun Wang, Fujuan Li, Shirley Ni, Lingling Xia, Zhenli Wang, Guangjun Liang. Research on blockchain consensus algorithm and application[J]. Computer Science and Exploration,2022,16(06):1214-1242.

[2] Zhou Hong ,Pan Ming. Metaverse opens a new era of digital collections [J]. Shanghai Informatisation, 2023, (08): 30-33.

[3] Qianqian Liu,Chenzhi He,Xiaoyang Chen et al. Digital Cultural and Creative Development of NFT Digital Collections and GLAM Institutions [J]. Library Construction, 2023, (03): 25-34+48. DOI:10.19764/j.cnki.tsgjs.20230847

[4] Jungwon S ,Sooyong P . SBAC: Substitution cipher access control based on blockchain for protecting personal data in metaverse [J]. Future Generation Computer Systems, 2024, 151 85-97.

[5] Ahmed M A A . A secure and privacy blockchain-based data sharing scheme in mobile edge caching system [J]. Expert Systems With Applications, 2024, 237 (PC):

[6] Xiaobo X ,Jin S . Research on the construction scheme of smart library based on blockchain technology [J]. Measurement: Sensors, 2024, 31

[7] Randa K ,El-Din E H ,Nawal E . Care4U: Integrated healthcare systems based on blockchain [J]. Blockchain: Research and Applications, 2023, 4 (4):

[8] Ibrahim Y A ,Alok M . Green blockchain – A move towards sustainability [J]. Journal of Cleaner Production, 2023, 430

[9] Usman K ,Ahmed O M ,Wee O H , et al. Leveraging a novel NFT-enabled blockchain architecture for the authentication of IoT assets in smart cities [J]. Scientific Reports, 2023, 13 (1): 19785-19785.

[10] Wang M ,Zhu J . Legal Issues Regarding Financial Data Security and Privacy Protection under Blockchain Technology [J]. The Frontiers of Society, Science and Technology, 2023, 5 (16):

AUTHORS

Li Sun received his master's degree from Southeast University. Currently, she is teaching in the School of Electrical and Computer Engineering, Chengxian College, Southeast University. Her research interests include computer science and technology, blockchain.

ZhiGang Han specializing in software engineering. His research interests include software engineering.

Zhulei Huang specializing in software engineering. His research interests include software engineering, blockchain.