

# Application of blockchain technology in the renovation management of old neighborhoods

Houhui Yu

Yunnan University of Finance and Economics, School of Information, Kunming 650221, China  
yhouhui@163.com.

**Abstract:** In the old neighborhood renovation process in the past, because of the large amount of funds involved, cumbersome procedures and processes, many participating units and independent databases of different government departments, it directly leads to a series of problems such as the difficulty of data information integration. Blockchain has the characteristics of non-tampering, traceability and decentralization. In this context, applying blockchain technology to the management process of old neighborhood renovation has become a new idea.

**Keywords:** Older neighborhoods; Blockchain; Renovation.

## 1. Overview of blockchain

Blockchain[1] is a new application model of computer technology such as distributed data storage, peer-to-peer transmission, consensus mechanism, and encryption algorithm. In a narrow sense, blockchain is a distributed ledger in which data blocks are sequentially linked in a chronological manner to form a chained data structure that is cryptographically guaranteed to be tamper-evident and unforgeable. Broadly speaking, blockchain technology is a new distributed infrastructure and computing method that uses a block-chain data structure to verify and store data, a distributed node consensus algorithm to generate and update data, a cryptographic approach to secure data transmission and access, and a smart contract composed of automated scripting code to program and manipulate data.

There are three main types of blockchains, namely public, private and federated chains[2].

A public chain is a completely open blockchain where participants can access the system at any time for data reading, trading, sending and confirming, competing bookkeeping[3], and system maintenance.

Alliance chain is a blockchain managed by several institutions, and is a hybrid blockchain between public and private chains; each institution runs and manages one or more nodes on the chain, and its data is only allowed to be read and written by institutions within the alliance, and institutions can send transactions and record transaction data together.

A private chain is a blockchain whose write access is controlled by an organization or institution, and whose read access can be open to the public or have a certain degree of restriction attached to it.

## 2. Blockchain technology

The technologies underlying blockchain include hash computing, digital signatures, P2P networks, consensus algorithms, and smart contracts[4,5].

### 2.1. Hash operation

Generate a fixed-length output from an input of arbitrary length by certain calculation, and the output string is the hash value of that input. Hash operation is characterized by fast

forward, sensitive input, difficult reverse and strong collision resistance, and the chain structure of blockchain is constructed through hashing to achieve tamper-proof.

The hash value of blockchain uniquely and accurately identifies a block, and each block header contains the hash value of the previous block data, so that the hashes are nested in layers, and eventually all blocks are linked together to form a blockchain. And tampering with a transaction means that all the block headers of all the blocks after it should be tampered with once, which is actually unattainable because everyone has a ledger, and only nodes controlling 51% or more of the computing power of the whole network can possibly tamper with historical transaction information.

The Merkle tree in the blockchain is a hash of all the transaction information of the current block. The hash is calculated for each transaction, and then grouped two by two, and the two hashes are then calculated to get a new hash, and the two old hashes are used as the leaf nodes of the new hash, until finally only one hash remains, which is the root of the Merkle tree, the root hash.

If the content of the transaction needs to be verified, it is only necessary to verify the Merkle tree. If the root hash verification fails, the two leaf nodes are verified, and then the leaf node of the node whose hash verification fails is verified, which can finally identify the tampered transaction accurately and achieve the purpose of rapid detection and location of the changed content.

### 2.2. Digital Signature

Blockchain uses digital signature to realize authority control, identify the legitimate identity of transaction initiator and prevent malicious node identity impersonation; digital signature is an algorithm to achieve the effect similar to traditional physical signature.

Usage of digital signature in blockchain: In the blockchain network, each node has a public-private key pair. When a node sends a transaction, it first signs the content of the transaction with its own private key, attaches the signature to the transaction and broadcasts it, and after other nodes receive the broadcast message, they first verify the digital signature attached to the transaction, and after completing the message integrity check and the legitimacy check of the identity of the message sender, the transaction will trigger the subsequent

processing process only after the message integrity verification and the message sender identity legitimacy verification are completed.

### 2.3. P2P network

Blockchain systems commonly use P2P network communication technology for broadcasting transaction information. P2P peer-to-peer networks are a distributed application architecture for distributing tasks and workloads among peers, and are widely used in various areas of computer networks, such as: file sharing, distributed computing, and voice instant messaging.

The advantages of P2P network technology are mainly reflected in decentralization, robustness, scalability, and privacy protection. In blockchain, resources and services in the network are scattered on each node, and information is directly transmitted to each other through each node without the need of a centralized server for forwarding. Since the transmission of information is dispersed among the nodes, when one or more nodes of the network are maliciously attacked or damaged, it does not affect the normal operation of the overall network of the blockchain, thus naturally ensuring the robustness of the P2P network.

### 2.4. Consensus algorithm

Blockchain solves the trust problem through universal bookkeeping, where all nodes participate in recording data. There are currently four types of consensus algorithms, proof-of-work class, credential class, Byzantine fault-tolerant class and consensus algorithms that incorporate a trusted execution environment.

### 2.5. Smart Contracts

Smart contracts are a milestone in the development of blockchain. Blockchain applications in finance, government services, supply chain, and gaming are all in the form of smart contracts that run on different blockchain platforms.

A smart contract is a set of commitments defined in digital form, including a protocol on which contract participants can execute these commitments, which is simply a computer program that executes automatically when certain conditions are met.

## 3. Blockchain working principle

Data structure of blockchain: Block is the basic unit of chain structure, mainly containing two parts, block header and block body. Block header consists of parent block hash value, timestamp, Merkle root (root hash) information; block body contains a list of string of transactions. The hash value of the parent block stored in the block header of each block uniquely specifies the parent block of that block, which constitutes a connection relationship between the blocks, which is the basic data structure of the blockchain.

The main work of blockchain is to transmit, verify, and pack the transactions issued by user nodes into data blocks, which are connected in chronological order to form a chain of data blocks. In this process, the nodes that have obtained the right to record, store and verify the transaction information, which can ensure the consistency of the consensus ledger data on the blockchain, prevent tampering, and prevent the account from "double spend". The specific working process is as follows.

(1) After a user node initiates a transaction, the transaction will be broadcast on the blockchain network, and other nodes

will receive the transaction information and put it into the transaction pool of their respective nodes.

(2) The miner node will package the transaction information in the local transaction pool and encapsulate the block according to the structure of the block, generating the block header and block body respectively.

(3) Depending on the consensus mechanism of the blockchain, miners get bookkeeping rights differently. A blockchain network using the Bitcoin system as an example uses the proof-of-work (POW)[6] mechanism, where the miners' job is to solve a mathematical puzzle and the first miner to solve it gets the bookkeeping rights for the block; in the case of a blockchain using the proof-of-stake (POS)[7] mechanism, block wrapper verification is performed.

(4) After encapsulated, the block will be broadcast to the whole network through P2P network; after other nodes receive this block, they will verify the legitimacy of the block, such as: block number, hash value, block difficulty, and transaction list.

(5) If the block is approved by most of the honest nodes, the block will be connected to the final position of the blockchain, and the miner node that gets the bookkeeping right will be rewarded accordingly.

## 4. The problems faced by the transformation of old urban neighborhoods

Urban old neighborhood transformation scope: according to the provisions of the Ministry of Housing and Construction, built before December 31, 2000, the loss of maintenance and repair of serious loss of management, municipal facilities are not perfect, social service facilities are not sound, the residents have a strong will to transform the city or county old neighborhood.

Urban old district transformation content: three types of implementation of transformation: one is the infrastructure protection class, the main content includes flooding water treatment, housing waterproofing measures, repair and replacement of downspouts, septic tank cleaning, drainage pipe unblocking, water supply pipe maintenance repair, fire channel cleaning, additional units of firefighting facilities, water and electricity a household meter transformation, gas pipeline laying into the household and finishing, street lights and building lighting, road repair The second is the infrastructure upgrading category. The second is the infrastructure improvement category, the main content includes building guardrail repair and cleaning, building wall painting, community building identification, overhead line cleaning, unit security door repair and replacement, housing facade painting, community security monitoring settings, additional sanitation facilities, motorized non-motorized parking area, roof solar transformation, community greening enhancement. The third is to improve public services, the main content includes the setting of barrier-free access, public activity square construction, outdoor fitness equipment, elderly and childcare sites, library construction, community medical points, newspaper boxes, courier cabinets, other convenient facilities. Focus on the above to protect and enhance the infrastructure content of the transformation, the conditions to further improve the community public service functions.

Old neighborhood transformation expected goals: through the transformation of old neighborhoods, the basic solution to

the old urban neighborhoods buildings in disrepair, infrastructure, public construction is missing, property management is not sound and other issues, through the transformation of old urban neighborhoods, make up for the shortcomings of infrastructure support, enhance public service functions, strengthen community management, create a green and comfortable living environment for residents, and effectively transform the production and living environment of residents to achieve "clean, livable, safe and orderly" living environment of the community.

## 5. Blockchain technology in the old neighborhood renovation management

The hash calculation in blockchain guarantees that the information cannot be tampered with; asymmetric encryption technology, digital signature and timestamp can solve the problem of multi-party trust; authorization can solve the problem of data sharing. By building a "Union Chain" for the transformation of old neighborhoods, all parties with interests are pulled to the Union Chain, which can jointly build, jointly use and jointly maintain the project, so that the use of funds is open and transparent, and the quality of the project is traceable, and the difficulty of coordination can be reduced, the efficiency of work can be improved, and the science of decision-making can be enhanced.

Blockchain technology is applied to the management of urban old neighborhood renovation, and the whole process of renovation is recorded. The smart contract function is used to make intelligent payment for the renovation money, solve the trust problem of multiple parties' participation, make timely payment, complete the renovation task with quality and quantity, and achieve the purpose of traceability afterwards.

With the help of blockchain technology, the project planning and design, project construction and implementation plan, project construction and transformation process, project bidding, project contract, project acceptance, project payment, and project long-term management process are standardized, and the "blockchain" technology is used to realize the whole process data record, so that the project data information cannot be tampered with or falsified.

The application of "blockchain" technology in the renovation management of old neighborhoods allows all documents, information, signatures and funds involved in the renovation to be recorded in the original. By using blockchain to store evidence and timestamp records, the time point of each act can be documented, and the credible timestamp records can be used to prove the authenticity of the document data, after which every access and change will be recorded and permanently stored on the blockchain to prevent the document data from being tampered. For project managers, time is saved, all information and documents can be easily searched, project classification is clear, capital control is clear and secure, various reports can be automatically output and regularly updated, data accuracy is improved, and work efficiency is enhanced. For the participants, they can submit the information electronically online to achieve the purpose of optimizing the business environment. For the people, blockchain deposition and timestamp records make every point of time of every act traceable. All documents, information, signatures and the destination of funds are recorded in the original, making the project transformation process fairer and more transparent, and reassuring the third-

party social input funds.

The use of blockchain technology allows the community to monitor the details of the use of funds, the bidding process of project construction, the project construction process, the project acceptance process, and the quality of the project can be traced back to its source at any time. Let everyone know clearly where the funds are going, know the quality of construction materials, know who designs, who constructs, who supervises, who quality checks, who manages, and create a good environment for the transformation of old neighborhoods.

General idea: Using blockchain technology, the results of all-important nodes are recorded in the whole process of old neighborhood renovation.

Blockchain technology is used to record the results of questionnaire survey of public opinion, "one courtyard, one policy" transformation plan, expert evaluation results, joint approval results of functional departments, bidding results, bidding control price/winning price, transformation construction drawing design, project establishment results, project progress, acceptance after transformation, payment of money during the whole transformation process and the management after the renovation are recorded. So that the transformation of each cell has a perfect record, and the results of each important step are chained, which strengthens the control of the process, and the use and payment of each fund are recorded to ensure the use of each fund in place. The whole transformation process can be traced during and after the transformation.

## 6. Conclusion

Applying blockchain technology to the project management platform of old neighborhood renovation, on the one hand, the information of personnel, materials and transaction amount is put on the chain through data encryption, which reduces unnecessary cost expenditure; on the other hand, in view of blockchain's characteristics of reliability and information non-tamper ability, all aspects of old neighborhood renovation process become clearer and more transparent, which increases the credibility of the government and at the same time reduces the public's consideration of old It also reduces people's worries about the quality of old housing renovation. The traceability of any part of the renovation process makes the whole project more convenient.

The continuous development of the Internet and information technology is changing the traditional business management mode of all industries. The introduction of blockchain technology in the government system is an inevitable trend of information technology change; blockchain technology is undoubtedly a credible means to solve the market fairness, effectively stopping the credit crisis at the root of endogenous credit, then promoting the optimization of industrial structure and improving the virtuous cycle of market operation, and promoting high-quality economic development.

## References

- [1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[J].
- [2] RU S J S and L. Survey of Blockchain Access Control in Internet of Things[J/OL]. Journal of Software, 2019, 30(6): 1632-1648. DOI:10.13328/j.cnki.jos.005740.

- [3] FANG X, DI M A, HOU W. Research on the Blockchain Consensus Mechanism for Distributed Renewable Energy Access[J/OL]. Zhejiang Electric Power, 2019. [http://en.cnki.com.cn/Article\\_en/CJFDTOTAL-ZJDL201907001.htm](http://en.cnki.com.cn/Article_en/CJFDTOTAL-ZJDL201907001.htm).
- [4] Szabo N. Smart contracts: building blocks for digital markets[J]. EXTROPY: The Journal of Transhumanist Thought,(16), 1996, 18(2): 28.[J].
- [5] ZHOU S, SHENG H, MA J. Review of the Application of Blockchain Technology in Traditional Chinese Medicine Field[C/OL]//ISAIMS 2020: 2020 International Symposium on Artificial Intelligence in Medical Sciences. 2020. <http://dl.acm.org/doi/pdf/10.1145/3429889.3429932>.
- [6] The Bitcoin Backbone Protocol: Analysis and Applications | SpringerLink[EB/OL].. [https://link.springer.com/chapter/10.1007/978-3-662-46803-6\\_10](https://link.springer.com/chapter/10.1007/978-3-662-46803-6_10).
- [7] KING S, NADAL S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[J/OL]. 2012. [http://www.researchgate.net/publication/265116876\\_PPCoin\\_Peer-to-Peer\\_Crypto-Currency\\_with\\_Proof-of-Stake](http://www.researchgate.net/publication/265116876_PPCoin_Peer-to-Peer_Crypto-Currency_with_Proof-of-Stake).