International Journal of Smart Business and Technology
Vol.6, No.2 (2018), pp.31-38
http://dx.doi.org/10.21742/ijsbt.2018.6.2.04

Research on Automatic Commodity Trading Method Based on Smart Contract

Adewale Amoo

Ladoke Akintola University of Technology, Nigeria
Adewale.amooli@yahoo.com

Abstract

Blockchain is a network-based technical solution for distributed ledgers collectively maintained through decentralization and trustlessness. A smart contract is the most representative blockchain application from the 1.0 stage to the 2.0 stage, and it plays an important role in the construction of decentralized applications. According to the characteristics of blockchain without center and trustlessness, this article designs a commodity transaction smart contract based on blockchain technology. The release and execution of the smart contract in this article are implemented on the Ethereum private chain, and Ethereum's transfer and payment functions are executed through the lightweight wallet plug-in Metamask of the Chrome browser. The execution of the smart contract is tested in the test network, and the operation of the smart contract is completed in the form of gas payment. Gas is the calculation work measurement for executing transactions in Ethereum, and there is a conversion relationship with Ether. The more gas is paid when each contract is executed, the higher the chance of being packaged and stored first. The transaction model proposed in this paper realizes the system's decentralization; the transaction and contract information are open, transparent, and non-tamperable, and the contract is automatically stored and executed. This design can significantly increase the transaction speed and gradually reach the performance of a centralized network. And providing an enterprise-level blockchain operating system makes application development and deployment easier.

Keywords: *Blockchain, Ethereum, Smart contract*

1. Introduction

In March 2018, the market value of Bitcoin exceeded $11,000, making Bitcoin a hot spot once again, and various tokens based on blockchain technology have sprung up due to this enthusiasm. Although Bitcoin and some similar tokens in the market are still controversial in the currency field, blockchain technology, the core technology of Bitcoin, is gradually accepted and recognized by people. From Bitcoin to programmable finance and then to the programmable society of the future, a non-centralized blockchain network continues to develop rapidly amidst controversy.

Blockchain is a network-based technical solution for distributed ledgers collectively maintained through decentralization and trustlessness. Its development can be divided into three stages: Blockchain 1.0 stage is represented by Bitcoin, which provides a non-Turing complete scripting language. Blockchain 2.0 is programmable finance represented by

Article history:
Received (June 9, 2018), Review Result (July 23, 2018), Accepted (September 6, 2018)

Print ISSN: 2288-8969, eISSN: 2207-516X IJSBT

Ethereum [1]. A smart contract is its representative application, and it gives Turing's complete programmable language Solidity, which expands the application range of blockchain. The future blockchain 3.0 will be a programmable world, including various decentralized applications and organizations [2][3].

The smart contract is the most representative application of the blockchain from the 1.0 stage to the 2.0 stage, and it plays an important role in the construction of decentralized applications. A smart contract is a concept proposed by Szabo in 1994 [4], which automatically executes a contract between two or more parties through a computer agreement and interface, thereby eliminating disputes over contract terms.

The concept of blockchain was born in 2008. Satoshi Nakamoto is on the website metzdowd. A paper called Bitcoin: A Peer-to-Peer Electronic Cash System, published on the com's cryptography mailing list, mentioned blockchain technology for the first time [5]. He used blockchain technology to construct Bitcoin (Bitcoin), The basic technology of data structure and encrypted transmission of transaction information. Although the legitimacy of Bitcoin has not been affirmed, blockchain, the core technology of Bitcoin, has attracted widespread attention at home and abroad. In January 2016, the British government released a special research report on blockchain [6].

In recent years, the rapid development of blockchain technology has attracted the participation of many institutions. In foreign countries, financial institutions such as banks and securities have become the main research force, and governments, regulatory agencies, traditional large enterprises, and emerging start-ups have also participated in full swing.

In the financial field, the Nasdaq in the United States, the American Depository Trust and Settlement Corporation, the Australian Stock Exchange, the European Bank for Clearing, Goldman Sachs, UBS, etc., have all explored blockchain technology. Also, a related blockchain financial laboratory has been established to research the application of blockchain online payment, electronic money, and settlement.

At the national level, the United Kingdom, Russia, the European Central Bank, etc., began to research the application of blockchain technology in electronic currency, securities, and payment and settlement in 2016.

Regarding technology companies, IBM and Microsoft started researching distributed ledger technology in 2015. They conducted a technical design for blockchain applications, providing usable application scenarios and ecosystems.

Some international cooperation organizations have also established related blockchain alliances, such as the R3 CEV alliance, Hyperledger, etc. Many financial institutions around the world join these alliances. By developing blockchain technology in the banking industry, they explore establishing blockchain organizations for international financial payment and settlement and build enterprise-level open-source distributed Ledger framework.

2. The development of blockchain technology

The blockchain maintains internal consistency through a distributed consensus mechanism. The content of transactions is recorded in blocks, and each block is linked to a block by a hash value to form a chain structure. The miner obtains the address of the next block through calculation and receives a certain token reward while having the accounting authority. By paying a certain token as a cost, users can have the authority to keep accounts, write the transactions in the specified block address, and synchronize them to each node in the network. When someone tries to modify the result of a transaction that has occurred, it is necessary to modify the transaction information in all nodes. Otherwise, it will not pass the consistency check and cannot become a legal record. However, it requires a lot of calculations to modify the record information of all nodes, which is often difficult to achieve. Based on this feature of the blockchain, it can ensure that the recorded data cannot be tampered with. This is also an important application of the blockchain for account records in the financial field.

2.1. The architecture of the blockchain

Blockchain technology uses blockchain data structures to verify and store data, uses distributed node consensus algorithms to generate and update data, uses cryptography to ensure the security of data transmission and access, and uses intelligence composed of automated script codes. A new distributed infrastructure and calculation method in which contracts are used to program and manipulate data. The blockchain architecture mainly comprises six levels [7], as shown in Figure 1.

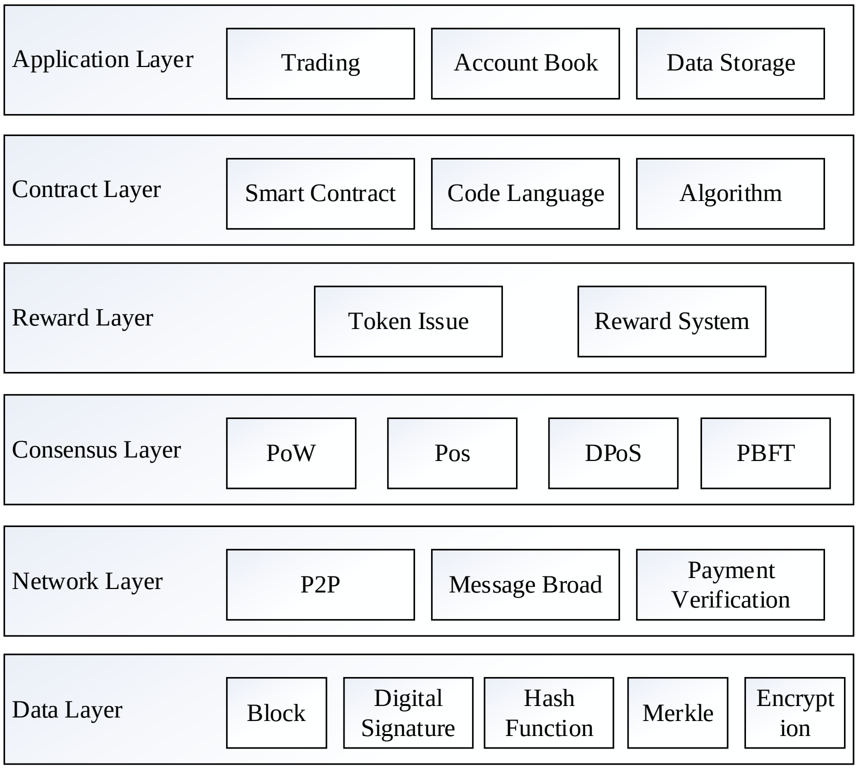

Figure 1. Blockchain structure

2.2. Representative blockchain applications

The applications based on blockchain technology have evolved from the initial Bitcoin to Ethereum to EOS (Enterprise Operation System), and new technologies are constantly being produced.

Bitcoin is the earliest blockchain application. It uses POW (Proof of Work Consensus Algorithm) to mine and generate new blocks by designing a non-centralized network. The miners continuously hash the block header and a random number through the double SHA256 encryption algorithm until a solution that matches the preset value appears. The miner who calculates the result first broadcasts this solution to the network. Verification and confirmation by other miners. After the verification is passed, it is added to the chain as a new block. While receiving the mining reward, the miner also obtains the authority to pack the transaction record into the new block and can charge the handling fee for the packaging transaction. To adapt to the increase in computing power and ensure that a new address is calculated every 10 minutes, the Bitcoin network will continuously adjust the difficulty of the calculation. When all 21 million Bitcoins are issued, the miners will rely on the package transaction fee. Maintain the power of mining.

Ethereum is the product of Blockchain 2.0. It uses POS to replace the POW of the Bitcoin network and replaces the weight of computing power with the amount of Ether it owns. In a POS system, the generation of new blocks of the blockchain is achieved through the participation of the coin holder or an influential coin holder in the system in the system. This is more efficient than POW mining, does not require high-performance hardware, and does not need to spend more electricity.

The most significant difference between Ethereum and Bitcoin is that Ethereum can support a more powerful scripting language, allowing developers to develop any application on it and implement any smart contract. Ethereum is like Apple's application store. Any developer can develop applications on it and sell them to users. At present, each block of Ethereum can hold about 200 transactions. Based on the average block generation time of 15 seconds, the transaction processing speed of Ethereum can reach 13 transactions per second.

EOS is a new blockchain architecture that aims to achieve the performance expansion of distributed applications. It is called blockchain 3.0. EOS solves the delay and data throughput problems faced by Bitcoin and Ethereum through parallel chains and DPOS. EOS can perform thousands of processing per second, transfer transactions, and run smart contracts on EOS, which does not need to consume system tokens. The share of tokens determines the bandwidth and computing power distribution of the EOS network. This means that if someone owns 1% of EOS tokens, he will always only get 1% of the network bandwidth, regardless of the load on the rest of the network.

Compared with Bitcoin and Ethereum, EOS focuses more on application. Bitcoin and Ethereum represent blockchain 1.0 and blockchain 2.0, respectively. The focus is on currency and smart contracts. EOS is to learn from and continue the previous ideas. Redevelopment represents the application-oriented blockchain 3.0.

By introducing three representative applications at different development stages of the blockchain, we can compare the aspects of the stage, function, consensus mechanism, block generation, transaction performance, programming language, etc., as shown in Table 1.

Table 1. Compare Bitcoin, Ethereum, and EOS

	Bitcoin (BTC)	Ethereum (ETH)	EOS
Stage	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0
Features	digital currency	smart-contract	application
Consensus mechanism	PoW	Now: PoW + PoS (Proof of Share) Future: PoS	DPoS (Proof of Entrusted Share)
The block generates	mining node	mining node	supernode
The transaction performance	<10	≈15	thousand, maybe reach millions
Programming language	UTXO	Solidity	C++/Rust/Python/ Solidity

3. Smart contracts

Smart contracts can be traced back to the mid-1990s when Nick Szabo predicted that the digital revolution would completely change how humans make contracts [8]. The conclusion of a smart contract can be recorded by implementing the agreed terms in computer code instead of daily language or legal language. Its work's basic principle is similar to a computer program's if-then statement. The corresponding contract clauses are automatically executed. Smart contracts are self-executing and self-enforcing. Only smart contracts can modify (add) ledger data. Simply put, a smart contract is a system that automatically transfers digital assets based on pre-established rules.

A smart contract is a set of agreements defined in digital form, including agreements on which contract participants can execute these agreements. The basic idea of smart contracts is that various contract terms can be embedded in the hardware and software used by people, so the attacker needs to pay a great price when attacking [9].

After the emergence of blockchain technology, its multi-party storage, multi-party calculation, transparent rules, non-tampering, and other characteristics just provide a safe and reliable record carrier and execution environment for smart contracts [10]. The smart contract is like an automatic agent living in the blockchain system. It has its blockchain address. When the user sends a transaction to the contract address, the contract is activated and established according to the settings. Every contract detail between the parties involved will follow the pre-written procedures. When a certain condition occurs, the terms in the contract are correctly executed, the contract will run its code and finally return a result, which may be another transaction sent from the contract address. At this stage, the smart contract technology represented by Ethereum has become a hot spot of concern from all walks of life. Ethereum supports Turing's complete development language to allow users to publish various smart contracts in Ethereum. The virtual machine Ethereum (EVM) provides is the operating environment of smart contracts. EVM provides an isolated operating environment as a sandbox to execute smart contracts [11]. The smart contract developed using the recommended programming language interprets the contract code into EVM bytecode through the EVM. Then, it is deployed on the blockchain after verification by the Ethereum network node. The deployment and execution of the smart contract are shown in Figure 2.

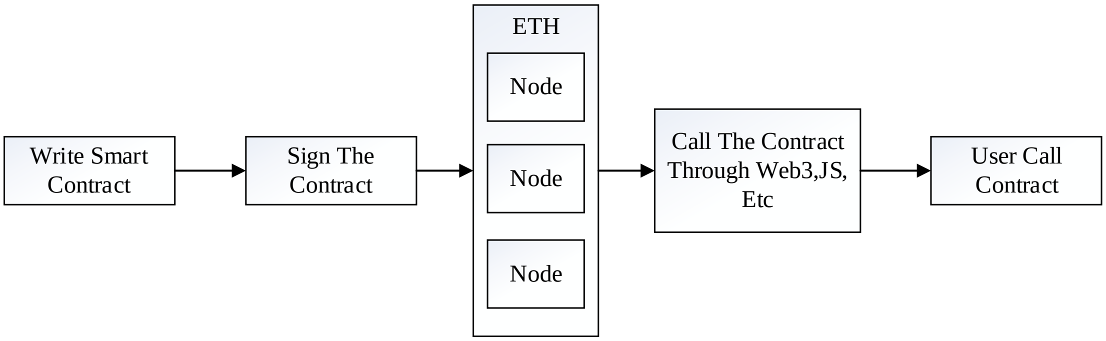

Figure 2. The deployment and execution of smart contract

4. Design of smart contract for commodity trading based on Ethereum

As a centralized e-commerce platform, although it provides a credible capital transaction environment for merchants and consumers, some problems will arise accordingly. Centralized e-commerce platforms need to play the role of mediation and arbitration between merchants and consumers. This will inevitably cause some disputes and consume platform resources. The decentralized commodity trading platform uses smart contracts to stipulate transaction behaviors between merchants and consumers. Both parties agree to the execution conditions of the smart contract. When the execution conditions are met, the platform automatically executes the agreed results of the contract to avoid disputes in the transaction. Since the smart contract is deployed in the blockchain and confirmed by the entire network through a consensus algorithm, it cannot be modified, avoiding some disputes caused by tampering with the contract's content.

Combined with the transaction process of traditional e-commerce, a smart contract model for commodity trading is designed, as shown in Figure 3. After merchants and consumers register as blockchain users, the blockchain will distribute public and private keys to each user. The public key is the user's account address on the blockchain, and the private key is the user's encryption key. Then, the two parties in the transaction agree on a smart contract that fits their needs. The two parties in the transaction use their private keys to sign and confirm the contact information to ensure the contract's authenticity and avoid malicious tampering. The contract's content is transferred to the blockchain through the P2P network, and the authentication node verifies the contract. After the consensus is completed, the legal contract is stored in the data block and executed automatically. This transaction model realizes the system's decentralization; the transaction and contract information are open, transparent, and cannot be tampered with, and the contract is automatically stored and executed.

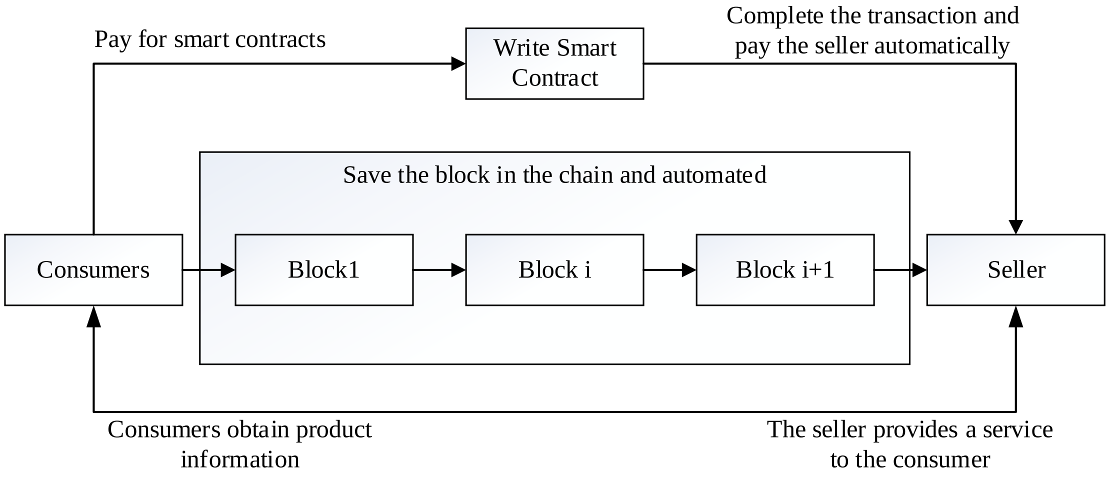
Pay for smart contracts
Write Smart Contract
Complete the transaction and pay the seller automatically
Save the block in the chain and automated
Consumers
Block1
Block i
Block i+1
Seller
Consumers obtain product information
The seller provides a service to the consumer

Figure 3. Smart contract trading model

According to the commodity trading smart contract model, combined with the traditional commodity trading process, the commodity trading smart contract algorithm is proposed. The algorithm flow is shown in Figure 4.

The specific steps of the algorithm are as follows:

Start:

Step1: Consumers query the merchant’s product information;

Step2: The consumer confirms the purchase of the product and sends the transaction information to the merchant;

Step3: Both parties to the transaction confirm the contract information and generate the contract;

Step4: The contract is generated, the consensus is completed in the chain, the execution function is imported into the block, and the liquidation is completed according to the end condition;

Complete contract execution.

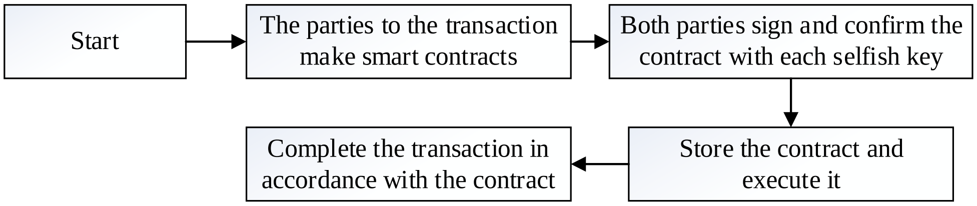
Start
The parties to the transaction make smart contracts
Both parties sign and confirm the contract with each selfish key
Store the contract and execute it
Complete the transaction in accordance with the contract

Figure 4. Smart contract trading algorithms

5. Conclusion

The issuance and execution of this smart contract are implemented on the Ethereum private chain, and Ethereum's transfer and payment functions are executed through the lightweight wallet plug-in Metamask of the Chrome browser. Among them, the merchant fills in the relevant product information data and submits the Metamask pop-up to pay the transaction fee. Then, the filled data will be forwarded to the MySQL database on the server side for storage. Consumers query related product information according to the ID of the smart contract issued by the merchant and transfer and pay through Metamask. The smart contract completes the transaction by calling the logistics signature information or the consumer's confirmation receipt information.

The execution of the smart contract is tested in the test network, and the operation of the smart contract is completed in the form of gas payment. Gas is the calculation work measurement for executing transactions in Ethereum, and there is a conversion relationship with Ether. The more gas is paid when each contract is executed, the higher the chance of being packaged and stored first.

The issuance and execution of smart contracts must pay a certain amount of gas. As the Ethereum network becomes increasingly congested, the cost of executing smart contracts will increase, bringing economic pressure to smart contract owners.

As a blockchain that truly supports smart contracts and is widely recognized, Ethereum has made great progress in the consensus algorithm compared with the Bitcoin era, and the speed of contract execution has also improved compared with the Bitcoin era, but it is relatively centralized. There is still a long way to go for the network's million-level TPS (Transaction Per Second) per second. In the future, blockchain 3.0 will greatly improve this situation. Taking the EOS network as an example, the transaction fee is no longer charged, and the transaction confirmation does not need to be approved by 51% of the entire network but is selected by voting. The super node will complete the block generation and accounting; in this way, the transaction speed will be greatly improved and gradually reach the performance of the centralized network. Providing an enterprise-level blockchain operating system will make the development and deployment of applications easier.

References

[1] M. Swan, “Blockchain: Blueprint for a new economy,” Sebastopol, CA: O’Reilly Media, Inc., **(2015)**

[2] M. Vasek, “The age of cryptocurrency,” Science, **(2015)**, vol.348, no.6241, pp.1308-1309

[3] H. Hodson, “Bitcoin moves beyond money,” New Scientist, **(2013)**, vol.220, no.2945, pp.24-24

[4] N. Szabo, “Smart contracts: Building blocks for digital markets,” EXTROPY: The Journal of Transhumanist Thought, no.16, **(1996)**

[5] A. Bahga and V. K. Madisetti, “Blockchain platform for the industrial internet of things,” Journal of Software Engineering and Applications, **(2016)**, vol.9, no.10, pp.533

[6] K. Bhargavan, A. Delignat-Lavaud, and C. Fournet, “Formal verification of smart contracts: Short paper,” Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. ACM, **(2016)**, pp.91-96

[7] Y. Hirai, “Defining the Ethereum virtual machine for interactive theorem provers,” International Conference on Financial Cryptography and Data Security. Springer, Cham, **(2017)**, pp.520-535

[8] J. Goldenfein and A. Leiter, “Legal engineering on the blockchain: Smart contracts as legal conduct,” Law and Critique, **(2018)**, vol.29, no.2, pp.141-149

[9] S. S. Gomes, “Smart contracts: Legal frontiers and insertion into the Creative Economy,” Brazilian Journal of Operations and Production Management, **(2018)**, vol.15, no.3, pp.376-385

[10] J. G. Allen, “Wrapped and stacked: Smart contracts and the interaction of natural and formal language,” European Review of Contract Law, **(2018)**, vol.14, no.4, pp307-343

[11] X. He, B. Qin, and Zhu, “Specs: A specification language for smart contracts,” IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, **(2018)**, vol.1, pp.132-137