Scientific Research Publishing

Open Journal of Applied Sciences, 2021, 11, 1135-1148
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Survey of Smart Contract Technology and Application Based on Blockchain

Somboun Tern

Guangxi University, Nanning, China
Email: aopaoo@hotmail.com

How to cite this paper: Tern, S. (2021) Survey of Smart Contract Technology and Application Based on Blockchain. *Open Journal of Applied Sciences*, **11**, 1135-1148.
https://doi.org/10.4236/ojapps.2021.1110085

Received: March 22, 2021
Accepted: October 26, 2021
Published: October 29, 2021

Abstract

With the vigorous development of blockchain technology represented by Bitcoin, blockchain technology has gradually surpassed the era of programmable currency and entered the era of smart contracts. Smart contracts are event-driven and stateful. With the in-depth development of blockchain technology, smart contracts use protocols and user interfaces to complete all steps of the contract process, allowing users to implement personalized code logic on the blockchain. Contract technology has the characteristics of decentralization, autonomy, observability, verifiability, and information sharing. It can effectively build programmable finance and programmable society, and is widely used in digital payment, financial asset disposal, multi-signature contracts, cloud computing, Internet of Things, sharing economy and other fields. First, it explains the basic concepts, full life cycle, basic classification, basic structure, key technologies, development status and main technology platforms of smart contracts; then discusses the application scenarios and development issues of smart contract technology, aiming to provide smart contract technology. The research and development provides reference.

Keywords

Smart Contract, Blockchain, Distributed Application, Formal Method, Crowdsale Contract

1. Introduction

Blockchain is the basic supporting technology of Bitcoin. With the rapid development and popularization of Bitcoin in recent years, it has attracted wide attention from many parties. In January 2016, the British government released a special research report on blockchain [1] in the same year. In September, the Chinese government included blockchain technology in the "Thirteenth Five-Year

Plan for National Informatization" [2], which aims to strengthen the basic research and development and cutting-edge layout of new technologies. Blockchain is considered to be the next generation of Internet computer technology. The fifth subversive innovation after, the Internet, and mobile social networks is the fourth milestone in the history of human credit evolution after blood credit, precious metal credit, and central bank banknote credit [3].

The application and development of blockchain technology has 3 stages: 1) Blockchain 1.0, which can program currency, such as Bitcoin; 2) Blockchain 2.0, which can program finance [4], of which smart contracts are its representative Application; 3) Blockchain 3.0, you can program the society, such as decentralized application (decentralized application), decentralized auto-nomous organization (decentralized auto-nomous organization) [4] [5]. At present, the blockchain has begun to surpass. In the era of blockchain 1.0, it has entered the era of blockchain 1.5 and transitioned to the era of programmable finance, that is, the era of smart contracts.

Since 2016, the smart contract technology represented by Ethereum [6] has become a hot spot of concern from all walks of life, and has attracted widespread attention from government departments, financial institutions, and technology companies. In December 2016, the first smart contract symposium Held at Microsoft's New York City headquarters, the application scenarios of smart contracts were analyzed and discussed. In February 2017, the European Parliament pointed out in the report "How Blockchain Changes Our Lives" [7] that smart contract technology is the most promising Blockchain application. In the same month, the Enterprise Ethereum Alliance was established to develop Ethereum into an enterprise-level blockchain. Its members include large financial institutions such as JPMorgan Chase and ABN AMRO, as well as Microsoft, Intel, etc.

The concept of "smart contract" (smart contract) was born in 1995 and was first proposed by cryptographer Szabo [8]. He pointed out that "smart contracts promote the execution of contracts through the use of protocols and user interfaces." In essence, smart A contract is an event-driven, stateful computer program deployed on a shared distributed database. The working principle of the existing smart contract is similar to the If-Then statement of other computer programs [9]. The smart contract only works in this way. Ways to interact with real-world assets. When a pre-set condition is triggered, the smart contract executes the corresponding contract terms.

Szabo pointed out that computers can replace humans, machinery and equipment in one day for more complex digital asset transactions. One day in the future, these automatically executed programs may replace some experts or institutions that handle specific financial transactions. Although the development of smart contracts it is in its infancy, but its potential is obvious. It proceduralizes the complex relationship between contract participants, contract agreements, and participants and agreements. The current development of blockchain-based smart contract technology presents a trend of innovation-driven technology industry,

But academic research is relatively lagging. As of July 2017, a search using Wanfang Knowledge Service Platform as the Chinese data source and EI Village as the English data source showed that the current title contains "smart contract/ smart contract" and is related to contents. There are only 9 academic papers related to blockchain technology in Chinese and 27 in English.

The content of this article has 6 aspects: 1) A brief introduction to the underlying technical basis of smart contracts-blockchain technology, and an overview of the definition, full life cycle, advantages and classification of smart contracts; 2) Concise summary of the basic structure of smart contracts, Key technologies; 3) Briefly introduced the main technology platform of smart contracts; 4) Summarized the existing problems of smart contracts; 5) Summary and outlook.

2. Background Knowledge of Smart Contracts

2.1. Introduction to Blockchain Technology

Blockchain technology originated in 2008 and was proposed by a scholar with the pseudonym "Satoshi Nakamoto" (Satoshi Nakamoto). The blockchain described in the literature is a chronological order of data blocks in a chain. The method is combined into a specific data structure, and a decentralized shared ledger (decentralized shared ledger) that is not tampered with and is guaranteed by cryptography [10]. Bitcoin is the earliest blockchain application scenario, and its essence is A distributed network based on blockchain technology uses cryptographic algorithms to generate digital cryptocurrencies. The field of digital cryptocurrencies has been facing two major problems: the double payment problem and the Byzantine generals problem [11]. Blockchain The emergence of technology provides an effective way to solve these two problems. The double payment problem refers to the use of "the same amount of money" to complete the payment in two or more transactions. The Byzantine Generals problem refers to the lack of a trusted central node. Under the circumstances, the problem of how to reach consensus and establish mutual trust in distributed systems [12]. Blockchain technology solves the problem of distributed databases, digital encryption technology and unique consensus algorithms without the need for third-party credit institutions. The double payment problem of a centralized system realizes a decentralized trustworthy system that does not need to trust a single node. The theoretical basis of the blockchain consensus algorithm is Byzantine fault tolerant (BFT). Common consensus algorithms have work. Proof of Work (PoW) [13], Proof of Stake (PoS) [14], Delegated Proof of Stake (DPoS) [15], Practical Byzantine fault tolerance (Practical Byzantine fault tolerance, PBFT) [16], delegated Byzantine fault tolerance (DBFT) [17], etc.

In a narrow sense, a blockchain is a data ledger shared by all nodes in a decentralized system. The block structure is shown in **Figure 1**. Each block is divided into two parts: a block header and a block body, involving chain structure, Hash algorithm, Technical elements such as Merkle tree and timestamp [18].

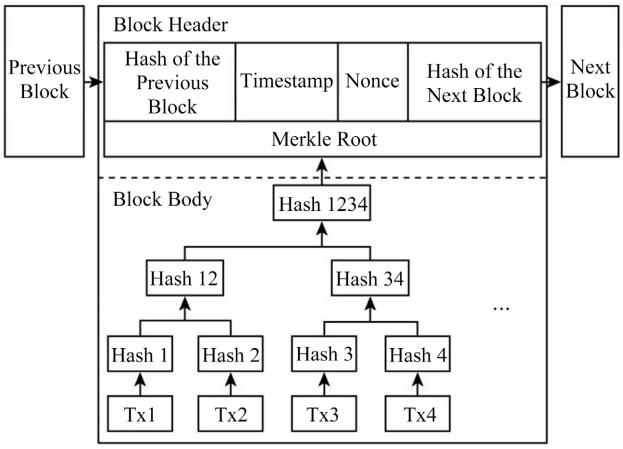

Figure 1. Structure of block.

The essence of blockchain technology is that it establishes a distributed consistency standard in the cyberspace, creates an exact record of all digital events that cannot be tampered with on the distributed database, and makes all participants in the blockchain Be able to accurately and credibly understand the digital events that have occurred.

After the emergence of blockchain technology, its characteristics such as decentralization, trustlessness, transparent rules, collective maintenance, and non-tampering provide a safe and reliable record carrier and execution environment for smart contracts. First of all, blockchain technology uses pure mathematics The method, without sacrificing privacy, and without the participation of third-party credit institutions, can establish a distributed consistent expression for all past and current digital events (such as behaviors, assets, etc.) [19]. Secondly, Blockchain provides a scripting system for users to program, which further enhances the flexibility of blockchain applications. For example, in Ethereum, it has a Turing-complete and powerful scripting system, making smart contracts more advanced Distributed applications are realized.

2.2. Smart Contract Overview

There are many informal definitions of smart contracts. Szabo creatively proposed that "smart contracts are computable transaction agreements that execute contract terms"; Ethereum's smart contracts are digital asset control programs based on blockchain [20]. In a narrow sense, a smart contract is a program code involving related business logic and algorithms, which proceduralizes the complex relationship between people, legal agreements, and the network. Broadly speaking, a smart contract is a computer protocol that can be deployed once it is deployed The realization of self-execution and self-verification is not only limited to the financial field, but also has broad application prospects in the fields of distributed computing and the Internet of Things.

Similar to a traditional contract, the full life cycle of a smart contract includes three parts: contract generation, contract issuance, and contract execution, as shown in **Figure 2**:

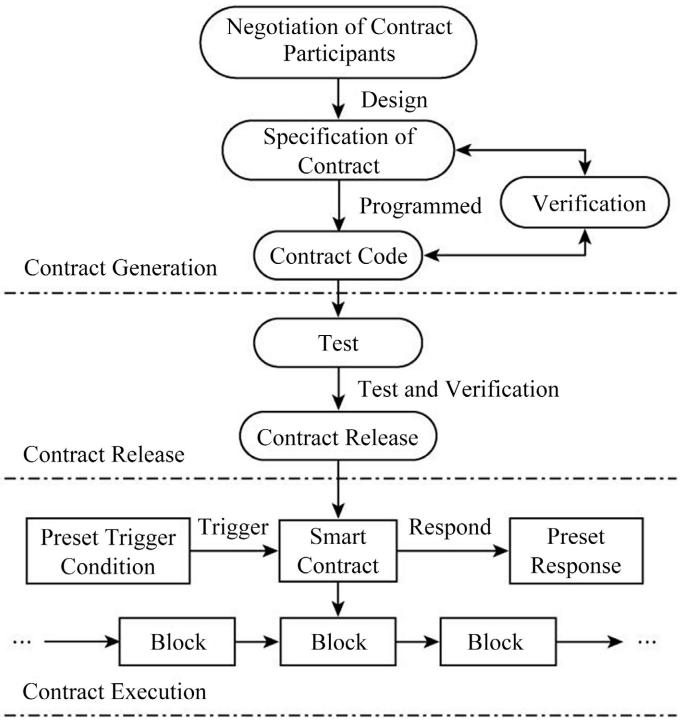

Figure 2. The whole life cycle of smart contract.

Contract generation mainly includes four links: contract multi-party negotiation, contract specification, contract verification, and contract code acquisition. The specific implementation process is: contract participants negotiate, clarify the rights and obligations of each party, determine the standard contract text, and The text is programmed, and the standard contract code is obtained after verification. There are two important links involved: contract specification and contract verification. Contract specifications need to be negotiated and formulated by experts with relevant field expertise and contract parties. Contract verification is based on the system abstract model. It is an important link related to the security of the contract execution process, and the consistency of the contract code and contract text must be ensured.

Contract release is similar to transaction release. The signed contract is distributed to each node through P2P, and each node will temporarily store the received contract in memory and wait for consensus. The realization of the consensus process: each node will The contracts temporarily stored in the recent period of time are packaged into a contract collection, and the hash value of the collection is calculated. Finally, the hash value of the contract collection is assembled into a block and spread to other nodes in the entire network; the block is received The nodes will compare and verify the Hash value stored in it with the Hash value of the contract collection they have saved; through multiple rounds of sending and comparison, all nodes will eventually reach a consensus on the newly released contract, and the consensus contract collection will be differentiated The form of the block spreads to the nodes of the entire network, as

shown in Figure 3. Each block contains the following information: the hash value of the current block, the hash value of the previous block, timestamp, contract data, and other descriptive information.

The execution of smart contracts is based on the "event trigger" mechanism. Blockchain-based smart contracts include transaction processing and storage mechanisms and a complete state machine for receiving and processing various smart contracts. Smart contracts will periodically traverse every node. The state machine and trigger condition of each contract will push the contract that meets the trigger condition to the queue to be verified. The contract to be verified will spread to each node. Like ordinary blockchain transactions, the node will first perform signature verification to ensure the contract. The validity of the verified contract will be successfully executed after consensus. The entire contract processing process is automatically completed by the smart contract system built into the bottom of the blockchain, open and transparent, and cannot be tampered with.

The realization of smart contracts is essentially by giving objects (such as assets, markets, systems, behaviors, etc.) digital characteristics, that is, the objects are programmed and deployed on the blockchain to become resources shared by the entire network, and then the contract is triggered by external events The automatic generation and execution of digital objects in the blockchain network will change the state (such as distribution, transfer) and values of digital objects. Smart contracts can actively or passively receive, store, execute and send data, as well as call smart contracts. Realize the control and management of digital objects on the chain. Smart contract technology platforms that have emerged, such as Ethereum, Hyperledger, etc., have Turing complete development scripting language, which enables the blockchain to support more smart contracts for financial and social systems application.

As far as the current development is concerned, smart contracts based on blockchain technology can be roughly divided into three categories: 1) "Chaincode", which is commonly referred to as on-chain code, such as financial activities from exchanging data to exchanging code; 2)" "Smart legal contracts" include rights and obligations arising from different aspects and are legally enforceable. They are usually expressed in complex legal texts. They not only cover personal behavior, but may also involve a series of dependencies such as time

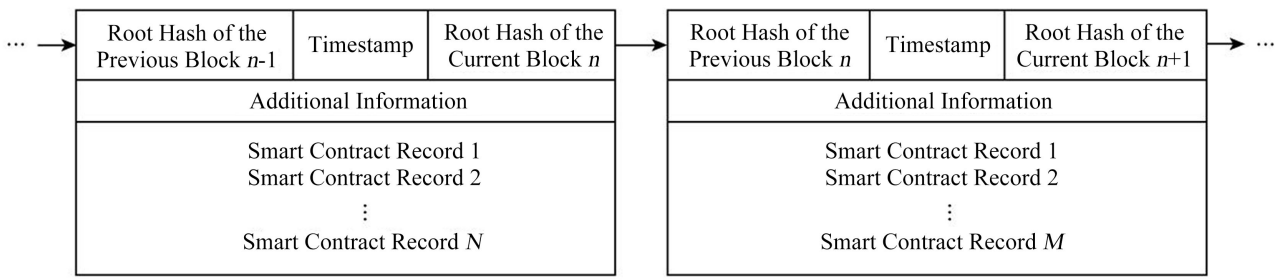

Figure 3. Blockchain diagram of smart contract.

dependence and order dependence. For example, PrimaveradeFilippi's legal framework for encrypted ledger transactions [21] uses on-chain smart contracts to supplement or replace existing legal contracts, which become a combination of smart contract code and traditional legal language; 3) "smart application contracts", that is, on the blockchain Deploy distributed on-chain applications based on smart contracts to create new forms of contracts with commercial value, such as the M2M (machine-to-machine) business model.

3. The Basic Structure and Key Technologies of Smart Contracts

The basic structure of a smart contract is shown in Figure 4. In general, a blockchain smart contract includes six elements: data layer, transmission layer, smart contract body, verification layer, execution layer, and application layer above the contract. The data layer includes On-chain data and off-chain data are necessary

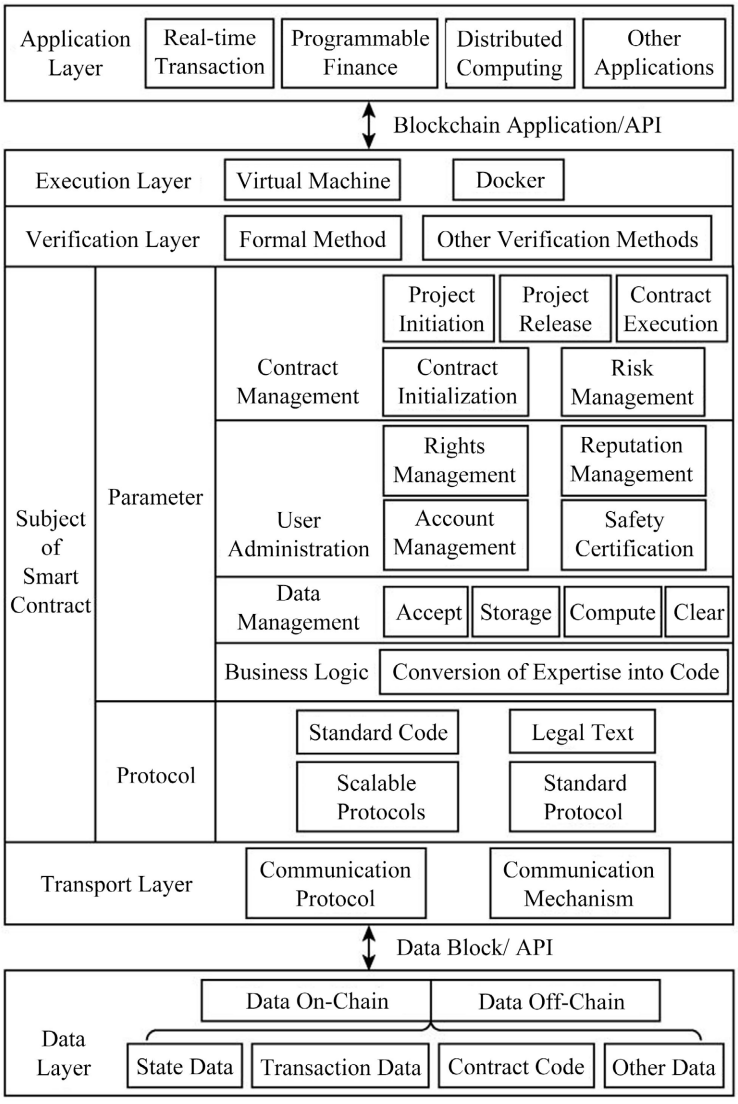

Figure 4. Basic framework of the smart contract.

data sources for the operation of smart contracts. The transport layer encapsulates the protocols used to support "on-chain-on-chain" and "on-chain-off-chain" communication and data transmission. Smart The main body of the contract includes protocols and parameters. The verification layer mainly contains some verification algorithms to ensure the consistency of the contract code and contract text. The execution layer mainly encapsulates the related software of the smart contract operating environment. The application layer is based on the first 5 elements. A variety of relatively advanced applications generated by the foundation, which are mainly used for communication between smart contracts and other computers and applications. This section will implement 5 aspects of smart contract subjects, data loading methods, execution environments, verification methods, and scalability. In terms of discussing the key technologies of smart contracts.

3.1. Smart Contract Overview

The smart contract subject provides a complex agreement framework for standardized contract applications, which can identify the behavior and status of the contract by identifying the key parameters of the smart contract. The smart contract subject mainly includes two parts: agreement and parameters:

1) An agreement is a procedural description of a legal text issued by a standards agency [22]. The agreement includes legal standard text and standard parameters, each of which has an identifier, which represents a type. It can be said that the agreement is a Fully instantiated template.

2) Parameters include business logic modules (main parameters) and various accessory modules, such as data management modules, user management modules, contract management modules, etc. Business logic modules include customized legal texts and parameters, which are programs for application domain expertise The description is generated by the contract participants through negotiation, involving the rights and obligations of multiple parties. The legal text and parameters of the business logic module come from the standard text and parameters of the agreement part, but vary according to the application scenario. The accessory module is the basis of the business logic The above, combined with the needs of specific application scenarios, realizes the supplement and improvement of smart contracts. The data management module encapsulates the code programs that realize the functions of data reception, temporary storage, calculation, and clearing; the user management module mainly realizes the contract users Authority management, security authentication, reputation management and other functions; contract management module, the main function is when the contract is called, combined with user needs, to achieve contract generation, verification release, deployment execution, status query and risk processing functions. Each module is based on Application requirements, you can customize sub-protocols and sub-standards, such as computing security standards, risk warning standards, module interaction protocols, etc. All parameters are a key part of the contract, because they not only directly reflect the business

relationship between the parties but also affect the contract Automatic execution.

3.2. Data Loading Method

The data layer includes state data, transaction data, contract code, application data, etc. For observable and verifiable purposes, state data and transaction data are generally stored on the chain. The loading methods of application data and contract code are divided into There are two types of on-chain and off-chain. At present, most blockchain systems use the on-chain method to publish code and application data to the chain, and then load and execute the data and code from the chain. The disadvantage is that the code and application The data will permanently exist in the blockchain, which is not conducive to update and maintenance, occupying node storage resources, and accumulating over time will bring a huge storage burden. The off-chain method refers to storing the hash value of the smart contract on the chain, And save the complete contract code through the storage network or trusted data source indexed by the hash value, such as IPFS (inter planetart file system) system, Tower Crier platform [23]. The hash value is determined by the content of the contract code. It is calculated, which can not only ensure the immutability of the contract, but also save a lot of storage space of the node and strengthen the privacy of the contract.

3.3. Execution Environment

At present, the mainstream smart contract execution environment design is mainly divided into two types: virtual machine and container (docker). Whether it is a virtual machine or a container, their role is to execute the contract code in a sandbox, and to use the contract Resource isolation and restriction. Virtual machine usually refers to the software implementation of a computer that has complete hardware functions and can execute programs like a real machine through software simulation, such as VMware. For the purpose of reducing resource overhead, improving performance and compatibility, the vast majority of blockchains will use a lightweight virtual machine structure, such as the Ethereum virtual machine (EVM). Containers usually refer to the use of container engines to allow developers to package their applications and dependent packages into a portable container, and can also be virtualized. Containers use a sandbox mechanism and there will be no interfaces between each other, such as Hyperledger Fabric. Use Docker as the execution environment of the smart contract. Docker itself does not use virtualization technology. The program runs directly on the underlying operating system, and the code execution efficiency is very high. However, compared with the lightweight virtual machine, its too large architecture. It requires a lot of time and computing resources to deploy and start Docker itself.

3.4. Implementation of Scalability

Scalability usually refers to how to handle larger-scale business. For the scalabil-

ity of a system, we usually have two methods, namely vertical expansion and horizontal expansion. Compared with horizontal expansion, vertical expansion is based on the maximum processing of a single device. The scalability of a capable serial system can easily reach the limits of cost and technology. Therefore, horizontal expansion is the mainstream measure at the moment, that is, the serial system is transformed into a parallel system and the instructions are processed in parallel.

The blockchain is essentially a distributed database that stores various data and the rules for the exchange and calculation of data, and smart contracts are the code implementation of these rules. Therefore, the concurrent execution of smart contracts will become an improved block An important approach to the scalability of the chain system, such as the sharding scheme proposed by Ethereum, that is, the nodes in the global validator set in the architecture are randomly assigned to specific "shards", where each shard handles the global state in parallel Different parts to ensure that the work is distributed across nodes.

4. Existing Problems of Smart Contracts

Although the blockchain-based smart contract technology has attracted many researchers with its unique advantages, the blockchain smart contract technology is still in the early stage of development and there are many problems. In addition, how to coordinate decentralization and low energy consumption. The relationship between security and security needs to be further studied. This section will discuss and analyze the issues to be resolved in the development of blockchain smart contract technology from the four aspects of efficiency, privacy, security, and standard inconsistency.

4.1. Efficiency Issues

Efficiency is an important factor affecting the availability of smart contracts.

1) Data storage problem. The smart contract block chain records all the state change records of the entire block chain network from its birth to the current point in time, and requires each node to save a data backup, which is great for the storage of ever-increasing massive amounts of data. It is extremely difficult to synchronize. For example, the Ethereum blockchain requires about 180 GB of storage space to fully synchronize all block data since the creation of the block. The newly added nodes to the network fully synchronize the data of the blockchain. It takes as long as 1 week. Although the Ethereum data block contains both smart contract code and transaction data, it has only been more than 3 years from its birth to the present. Even if the smart contract is separately chained, according to Ethereum's increasingly active trend and cumulative effect of time, its blockchain database is too large is an urgent problem to be solved. Although lightweight blockchain can partially solve this problem, most of the lightweight blockchain is at the expense of Reliability and safety come at the cost, so how to coordinate the relationship between lightweight and reliability and safety needs

further research. At the same time, industrial-grade solutions are still to be developed [24].

2) The efficiency of state confirmation. This mainly involves two problems: double confirmation and blocking. When different nodes with access rights modify the same state of the same smart contract, due to the existence of the time difference in the confirmation process, they will face "double confirmation" "The problem is that the same state is written 2 or more times, which may cause a state in the smart contract to be incorrectly modified or overwritten. For example, node 1 submits a modification request before node 2, but due to the time difference in the confirmation process. With the existence of, the application of node 2 may be confirmed before node 1, and when node 1 is confirmed, it will overwrite the modification of node 2 before. The "locking problem", that is, the priority of obtaining confirmation will produce the effect of locking the contract, so The contract denies access to other nodes. Ethereum can currently process 10 - 20 transactions per second, and to determine the transaction has to wait for the next block to be generated, with an average time of 12 s. So how to improve the ability of the blockchain to process transactions? It is an important problem to be solved urgently by blockchain smart contract technology. At present, researchers have begun to try to solve such problems, such as data sharding technology and indexing technology. Blockchain technology platform Zilliqa [25] proposed a sharing protocol based on The blockchain, which uses sharding technology, can process nearly 1400 transactions per second on the testnet. Although compared to the Ethereum blockchain, its transaction efficiency has been greatly improved, but for the deployment of a world-wide Large-scale smart contract projects that people participate in to deal with the stress resistance of large-scale transactions still lack a comprehensive solution to the efficiency problem.

4.2. Private Issues

Smart contract risk management and crisis response scenarios are not yet complete. At present, the privacy protection of smart contracts is based on the principle of asymmetric cryptography and has high security. However, with the further development of mathematical research and quantum computer technology, the future will be asymmetric Encryption algorithms may be cracked, and smart contracts still have weak links in terms of privacy and security.

According to the characteristics of blockchain technology, the privacy protection mechanism of blockchain can be divided into three categories: privacy protection at the network layer, privacy protection at the transaction layer, and privacy protection at the application layer [26]. At present, privacy protection is mainly through increasing. It is achieved by the difficulty of malicious nodes to retrieve, obtain and interpret blockchain data, such as the mimicry defense technology introduced by Professor Si Xueming's team, as well as network layer data obfuscation technology and data distortion technology. With the develop-

ment of blockchain technology. With each passing day, privacy protection issues will become more prominent, but the current privacy protection schemes have certain shortcomings, and further research is needed.

4.3. Security Issues

Traditional contracts are described based on natural language; while smart contracts use computer code to explain, verify, and execute contracts, which puts forward higher requirements for ensuring the security of digital assets and resources. Smart contracts will eventually replace contract entities, but as mentioned in section 2.4, smart contracts involve complex time dependence and order dependence. The uncertainty and inconsistency of the contract code will lead to loopholes in the smart contract itself, which will lead to uncertainty in the execution result of the contract and ultimately lead to legal liability. Uncertainty [27]. In May 2016, The DAO, one of the largest crowdfunding projects in history, had a loophole in the smart contract at the beginning of its design. The attacker used the "splitDAO" function in the DAO.sol code to exist in the recursive sending mode. A large amount of Ether was stolen from the vulnerability. On July 19, 2017, a vulnerability was discovered in the "multi-sig" code of Parity Wallet's multi-signature wallet, that is, the process of creating a multi-signature wallet is unprotected, making the attack The owner can reset the ownership and usage parameters of the existing wallet at will, which resulted in the theft of the 3 large Ether accounts in Parity Wallet. Therefore, the smart contract must ensure the correctness of its logical attributes and the correctness of the contract code and contract text. Consistency, and can automatically generate trusted execution code. At present, scholars or groups have proposed verification methods for smart contracts, such as the OYENTE semantic notation tool, but it is not yet complete. There are still many logics about smart contracts. The issues of integrity, verifiability, and security need to be studied and explored in depth.

5. Summary and Outlook

Since the birth of Bitcoin in 2009, the blockchain technology represented by it has risen rapidly and has become a hot research topic in academia and industry. It has experienced the era of blockchain 1.0 represented by digital currency. The research direction of the blockchain will be based on "blockchain 2.0 applications, supplemented by blockchain 3.0 applications". Blockchain 2.0 is the era of smart contracts, which can adapt to more complex application scenarios and more advanced functional requirements, making it have a wide range of application prospects in financial and social systems; at the same time, other advanced applications based on smart contracts also have vigorous development potential. Smart contract technology is expected to become the realization of the Internet of Things, large transaction volume blockchain, and decentralization. It forms an effective way of cloud storage and decentralized name servers.

At present, the basic theory and technical research of smart contract technol-

ogy is still in its infancy, and there is still a lack of research and exploration on basic theories, key technologies, and scientific issues that are vital to the development of the industry. There are many challenging problems in this field. See the 4 aspects introduced in Section 5. It should be pointed out that for the challenging problems faced by smart contracts, this article only selects a representative part of them to introduce or summarize, and does not cover all research directions and problems.

This article systematically introduces the full life cycle, basic architecture, key technologies, research status, main technology platforms and application scenarios of smart contract technology, and discusses possible problems. It is a summary of the current research results of smart contract technology. At the same time, a crowdfunding contract system was developed to explore and practice the relevant theories of smart contracts. The original intention of this research field is to show the current research status and cutting-edge issues of smart contract technology, so as to provide references for scholars in related fields.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Hancock, M. and Vaizey, E. (2017) Technical Report by the UK Government Chief Scientific Adviser. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[2] National Development and Reform Commission (2017) The Thirteenth Five-Year National Informatization Plan. http://www.xinyifanyi.com/news.asp?id=13709

[3] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., Sebastopol, CA.

[4] Vasek, M. (2015) The Age of Cryptocurrency. *Science*, **348**, 1308-1309. https://doi.org/10.1126/science.aab2001

[5] Hodson, H. (2013) Bitcoin Moves beyond Money. *New Scientist*, **220**, 24. https://doi.org/10.1016/S0262-4079(13)62791-8

[6] Buterin, V. (2017) A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper

[7] Philip, B. (2017) How Blockchain Technology Could Change Our Lives. http://8btc.com/doc-view.html?d=1319

[8] Szabo, N. (2017) Formalizing and Securing Relationships on Public Networks. http://www.firstmonday.org/ojs/index.php/fm/article/view/548/469

[9] He, P., Yu, G., Zhang, Y.F., *et al.* (2017) Survey on Blockchain Technology and Its Application Prospect. *Computer Science*, **44**, 1-7.

[10] Antonopoulos, A.M. (2014) Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media Inc., Sebastopol, CA.

[11] Swan, M. (2015) Blockchain Thinking: The Brain as a Decentralized Autonomous Corporation. *IEEE Technology & Society Magazine*, **34**, 41-52.

https://doi.org/10.1109/MTS.2015.2494358

[12] Dwork, C. and Naor, M. (1992) Pricing via Processing or Combatting Junk Mail. In: Brickell, E.F., Ed., *Advances in Cryptology—CRYPTO*'92, Springer, Berlin, 139-147. https://doi.org/10.1007/3-540-48071-4_10

[13] Larimer, D. (2017) Transactions as Proof-of-Stake.

[14] Larimer, D. (2017) Delegated Proof-of-Stake White Paper. http://8btc.com/doc-view-151.html

[15] Castro, M. and Liskov, B. (2002) Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems*, **20**, 398-461. https://doi.org/10.1145/571637.571640

[16] NEO Smart Economy (2018) NEO White Paper. https://neo.org/event/details/1

[17] Bitcoin (2017) Bitcoin Core Integration. https://github.com/bitcoin/bitcoin

[18] Yuan, Y. and Wang, F.Y. (2016) Blockchain: The State of the Art and Future Trends. *Acta Automatica Sinica*, **42**, 481-494.

[19] Hu, K., Bai, X.M., Gao, LC., *et al*. (2016) Formal Verification Method of Smart Contract. *Journal of Information Security Research*, **2**, 1080-1089.

[20] Wright, A. and De Filippi, P. (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network*, **34**, 41-52. https://doi.org/10.2139/ssrn.2580664

[21] Clack, C.D., Bakshi, V.A. and Braine, L. (2017) Smart Contract Templates: Foundations, Design Landscape and Research Directions. https://arxiv.org/abs/1608.00771

[22] Zhang, F., Cecchetti, E. and Croman, K., *et al*. (2016) Town Crier: An Authenticated Data Feed for Smart Contracts. *Proceedings of the* 2016 *ACM SIGSAC Conference on Computer and Communications Security*, New York, October 2016, 270-282. https://doi.org/10.1145/2976749.2978326

[23] Chen, W.L., Yang, Z.H., Zhang, D.M., Huang, Z.Q., Song, F. and Wang, L. (2012) Reconstruction of Major Full Cheek Defects with Combined Extensive Pedicled Supraclavicular Fasciocutaneous Island Flaps and Extended Vertical Lower Trapezius Island Myocutaneous Flaps after Ablation of Advanced Oral Cancer. *Journal of Oral & Maxillofacial Surgery*, **70**, 1224-1231. https://doi.org/10.1016/j.joms.2011.06.208

[24] Kenneth, M. (1996) Symmetry and Model Checking. *Formal Methods in System Design*, **9**, 105-131. https://doi.org/10.1007/BF00625970

[25] D'Silva, V., Kroening, D. and Weissenbacher, G.A (2008) A Survey of Automated Techniques for Formal Software Verification. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **27**, 1165-1178. https://doi.org/10.1109/TCAD.2008.923410

[26] Frantz, C.K. and Nowostawski, M. (2016) From Institutions to Code: Towards Automated Generation of Smart Contracts. 2016 *IEEE* 1*st International Workshops on Foundations and Applications of Self* Systems* (*FAS*W*), Piscataway, 12-16 September 2016, 210-215. https://doi.org/10.1109/FAS-W.2016.53

[27] Zhang, Y.B., Gong, Z.H. and Wang, L.C. (2004) Research and Implementation of LDP Conformance Testing. *Computer Engineering and Science*, **26**, 14-16.