Wireless Networks (2022) 28:635–690
https://doi.org/10.1007/s11276-021-02874-x

ORIGINAL PAPER

A survey of application research based on blockchain smart contract

Shi-Yi Lin[1] · Lei Zhang[1] · Jing Li[1] · Li-li Ji[2] · Yue Sun[1]

Accepted: 13 December 2021 / Published online: 17 January 2022

Abstract
Nowadays, blockchain technology and industry has developed rapidly all over the world, which is inseparable from continuous innovation and improvement on smart contract technology. Therefore, by summarizing the working principle and application research status of blockchain smart contract, this paper analyzes the development and challenges of smart contract. Firstly, we introduce the model and operation principle of blockchain smart contract for the overall architecture, analyze the deployment process of smart contract with Ethereum, Hyperledger Fabric and EOSIO, and make a comparative analysis from the technical level. And taking Byteball, InterValue and IOTA platforms as examples, we introduce the deployment process and application potential for DAG-based blockchain smart contract. Additionally, we also summarize the application research of smart contract for international and Blockchain Oracle, and discuss its innovative application and development trend in the future. Secondly, we introduce the application status of smart contract with Ethereum and Hyperledger Fabric platforms from the aspects of financial transactions, Internet of things, medical applications, and supply chain, and further discuss EOS (enterprise operation system), Blockchain Oracle and other application fields. Furthermore, we introduce the application advantages and challenges to smart contract for industrial Internet from the fields of manufacturing, food industry, industrial Internet of things and industry 4.0. Finally, we discuss the challenges faced by smart contract with technical issues, analyzes the impact on large-scale applications and mining system on the sustainable development of smart contract, and looks forward to the future research direction of blockchain smart contract.

Keywords Blockchain · Smart contract · Industry 4.0 · DAG-based blockchain · Industrial internet of things · Blockchain Oracle

1 Introduction

With the rapid development of cryptocurrencies such as Bitcoin and the application of blockchain technology in industries such as finance, Internet of things (IoT), cloud computing and supply-chain, blockchain has gradually attracted global attention [1]. Blockchain provides a programmable environment for smart contracts as an emerging technology with great potential. Taking advantage of blockchain, smart contract has been widely used in blockchain. Smart contract can not only change the existing business model, but also bring a lot of convenience to public life in reality.

The concept of "smart contract" was first proposed by Nick Szabo in 1995 [2], specifically defined as "a smart contract is a set of commitments defined in digital form, including the agreement that the participants in contract can implement these commitments". Smart contract is a computer protocol designed to disseminate, verify or execute contracts in an information-based manner. It allows trusted transactions without a third party and these transactions are traceable and irreversible, which purpose is to provide better security than traditional contracts and reduce other transaction costs related to contracts. Therefore, smart contract characterized by the high efficiency of development, lower maintenance cost and high accuracy of execution fit perfectly with the blockchain technology. It

✉ Lei Zhang
8213662@163.com

✉ Li-li Ji
jmsdxwk3019@163.com

[1] Collage of Information Science and Electronic Technology, Jiamusi University, Jiamusi 154007, Heilongjiang Province, China

[2] Science and Technology Department, Jiamusi University, Jiamusi 154007, Heilongjiang Province, China

can be said that smart contract is one of the key features of blockchain technology [3]. As a core technology of blockchain, smart contract based on blockchain has been widely used in blockchain projects with strong influence such as Ethereum and Hyperledger.

The emergence of blockchain technology defined smart contract and made it possible. Smart contract is an embedded programming contract that can be built into any blockchain data, transaction or asset to form systems, which to form systems, markets or assets controlled by the program [4]. It not only provides innovative solutions for the financial industry, but also plays an important role in the management of affairs as information, assets, contracts, supervision, and others in the social system.

According to the progressive history of blockchain technology, the development of smart contract can be divided into three stages, as shown in Fig. 1: in blockchain 1.0, the representative application is Bitcoin, which the contract for it is mainly used to achieve digital currency transaction, and its function is relatively single. And RSK (rootstock), the smart contract development platform based on bitcoin ecosystem, also needs to be highly compatible with Ethereum at present [5]. In blockchain 2.0, with the emergence of smart contract, DApp (decentration application) can be built on the blockchain, which the transaction speed and the system performance are improved, and the functions are diversified. According to the openness of blockchain, it can be generally divided into public blockchain and consortium (both private blockchain and consortium blockchain belong to the license blockchain, and private blockchain is a special form of consortium blockchain) [6]. Among them, the most representative development platforms are Ethereum and Hyperledger Fabric respectively. With the prosperity and development of blockchain ecology, new development platforms continue to make breakthroughs (such as side chain / cross chain technology, etc.) [7–9] to solve the current challenging problems and make full preparations for the arrival of blockchain 3.0. At the same time, they are also highly expected and disputed, and the most representative development platform is EOS. To sum up, Ethereum, Hyperledger Fabric and EOS are representative in terms of technology. Ethereum and Hyperledger Fabric are two core platforms for developing smart contracts at present, and analyzing their system architecture will help us understand the development principle of smart contract for the public blockchain and the consortium chain. The review of EOS will help us better understand the development trend of smart contract and trigger readers' thinking on the large-scale application of smart contract. In addition, these three platforms are also in a state of continuous development, from which we can understand how the blockchain technology led by smart contract can help the real economy to develop to a deeper level in a new way of cooperation.

In view of the decentralized nature of blockchain-based smart contracts and the nature of the contracts themselves, the applications of blockchain-based smart contracts can be divided into three categories from the technical level:

1. Ethereum. This is an open-source and universal public blockchain platform with smart contract function, which the point-to-point contract is processed through its special cryptocurrency Ether (ETH) and Ethereum

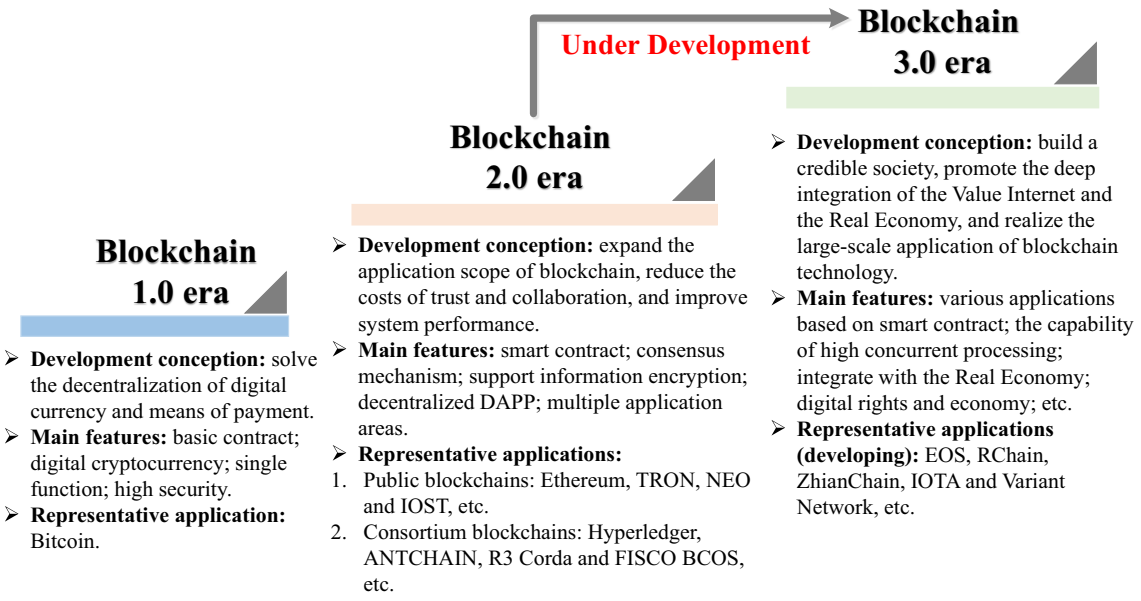


Fig. 1 The progressive history of blockchain smart contract

Virtual Machine (EVM) [10]. It can be used to create decentralized programs, autonomous organizations, and smart contracts, which its applications of goal cover fields such as finance, IoT, smart grid and sports quiz.

2. Hyperledger Fabric. This is a modular and open-source enterprise class licensed distributed ledger technology (DLT) platform, which is designed to be used in the enterprise environment. It mainly provides functions such as channels creation and pluggable implementation of different components [11]. Fabric has a highly modular and configurable architecture, which can provide innovation, flexibility and optimization for banking, finance, insurance, healthcare, human resources, supply chain and even digital music delivery industries.
3. Enterprise Operation System (EOS). This is a blockchain underlying public blockchain operating system designed for commercial distributed applications, which aims to solve the problems of low performance, poor security, high difficulty in development and excessive dependence on handling charges of existing blockchain applications, and to achieve the performance scalability of distributed applications [12]. The decentralized application of EOS mainly includes e-commerce, financial technology, and market.

Smart contract provides a programmable mechanism and flexible algorithm for bottom blockchain data, and lays the foundation for building blockchain 2.0 programmable financial system and blockchain 3.0 programmable social system, which will help to promote the application of blockchain technology in various distributed artificial intelligence systems [13]. Smart contract was unable to process the data with complex logic and high throughput in the application, and lacks privacy protection as well due to the performance limit of blockchain system. Therefore, it is of great significance to analyze the shortcomings of smart contract based on blockchain in the application and study the targeted solutions. At present, there have been many applications of blockchain smart contract with technical contributions to a certain extent. Although smart contract had obvious advantages over traditional contract, the in-depth research and application of it had still in the stage of continuous exploration, and the potential risks of emerging technologies still exist.

This paper is intended to summarize the current research results of application of blockchain smart contract on the technical level. Based on ordering the knowledge of smart contract, the paper discusses the deficiency of the existing research results, which looks forward with the development trend and prospect of smart contract, and hopes to provide useful help and inspiration for the future research on key technologies of it.

2 Background knowledge of smart contract application

Nick Szabo's working theory about smart contract has been slow to realize, which one of the important reasons is the lack of digital systems and technologies that can support programmable contract [3]. The emergence of blockchain technology solves this problem. It can not only support programmable contracts, but also provide with the advantages of decentralization, tamper-proof, transparent-process and traceability, that's why it is well suited for the development of smart contract [14].

Blockchain technology is based on distributed consensus algorithm to generate and update data, which is several main types of consensus mechanisms now [15]: Proof of Work (Pow), Proof of Stake (Pos), Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPOS). Blockchain technology mainly ensures the security of data transmission and access through cryptography, which is one of the core parts of it. Currently, many classical algorithms of modern cryptography are used in the application of blockchain [16] including the Hash algorithm, symmetric encryption, asymmetric encryption, digital signature, etc. Which among them, Secp256k1, an Elliptic Curve Digital Signature Algorithm (ECSDA), is the most commonly used digital signature algorithm. According to its functions, the infrastructure of blockchain [1] can be divided into three parts that form the architecture from bottom to top: infrastructure, protocol and extension, as shown in Fig. 2. The infrastructure part links the security of traditional network with blockchain security. In the protocol part, it realizes the corresponding functions based on the foundation system of hardware or network provided by the infrastructure layer. And these two parts provided the corresponding functions for the extension part to support services. Each part completes the core functions of its own, and each layer cooperates with each other, thus achieving the decentralized trust mechanism.

The infrastructure part consists of the data layer and the network layer. The data layer is the lowest level data structure of the whole blockchain technology. It encapsulates the chain structure of the underlying data blocks, as well as technologies such as asymmetric public private key data encryption and timestamp. Furthermore, its main functions are data and accounts storage based on Merkle tree, as well as the implementation and security of transactions [17]. The essence of blockchain is Peer-to-Peer (P2P) network that is nodes maintains communication by maintaining a common blockchain. However, the main

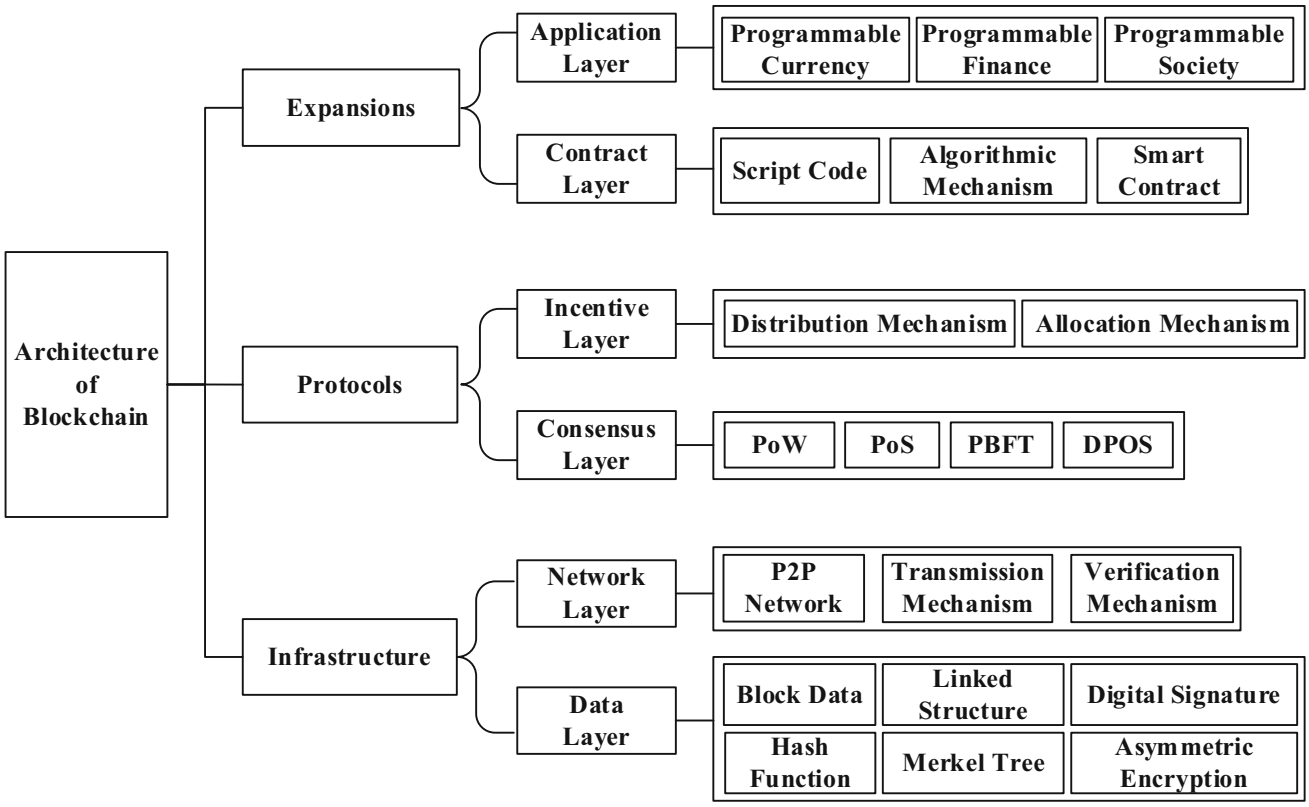


Fig. 2 The infrastructure of Blockchain

purpose of network layer is to achieve information interaction between nodes in the blockchain network, which includes P2P networking mechanism, data dissemination mechanism and data verification mechanism. The protocol part is mainly composed of the consensus layer and the incentive layer. The consensus layer is the basis and core of blockchain. Highly dispersed nodes can reach a consensus in the decentralized system through the consensus algorithm mechanism to jointly maintain the ledger. The incentive layer mainly includes the issuing mechanism and distribution mechanism of economic incentives. Its function is to provide incentive measures, which encourages nodes to participate in the safety verification of blockchain, so as to ensure the safe operation of the whole network, and mostly used in the public blockchain. The extension part consists of the contract layer and the application layer, which mainly provides diversified services and access by calling the functional components of the protocol part. As the basis of the programmable characteristics of blockchain, the contract layer encapsules all kinds of scripts, algorithms and smart contracts. Moreover, the smart contract is pieces of code running on the blockchain that can be automatically executed without intervention, mainly to implement algorithms and custom logic. The application layer encapsules various application scenarios and cases of blockchain, such as Cryptokitties [18] and DApp, and the future programmable society will also be built on the application layer.

The basic architecture of smart contract is shown in Fig. 3, and it is composed mainly of data-layer, transport-layer, the main body of smart contract, verification-layer, execution-layer and application-layer [19–21]. The data-layer is mainly responsible for storing the data on the blockchain, and interacts with the transport layer through the API, so that transferring the relevant data to the main body of smart contract. The transport-layer mainly encapsules the protocol that communication and data transmission with blockchain. The main body of smart contract includes two parts: protocol and parameters. Protocol is a procedural description of legal text issued by standard organization, and it is a fully instantiated template. As a key part of contract, parameters are mainly distributed in contract management, user management, data management and the business logic. The four parts in parameters directly reflect business-logic, and affect the automatic execution of contract, hence the main body of smart contract provides a complex protocol architecture for the contract of application based on standardization. The verification-layer mainly includes verification algorithm to ensure the validity of contract code and text. The execution-layer encapsules the software related to the running environment of smart contract to ensure the normal

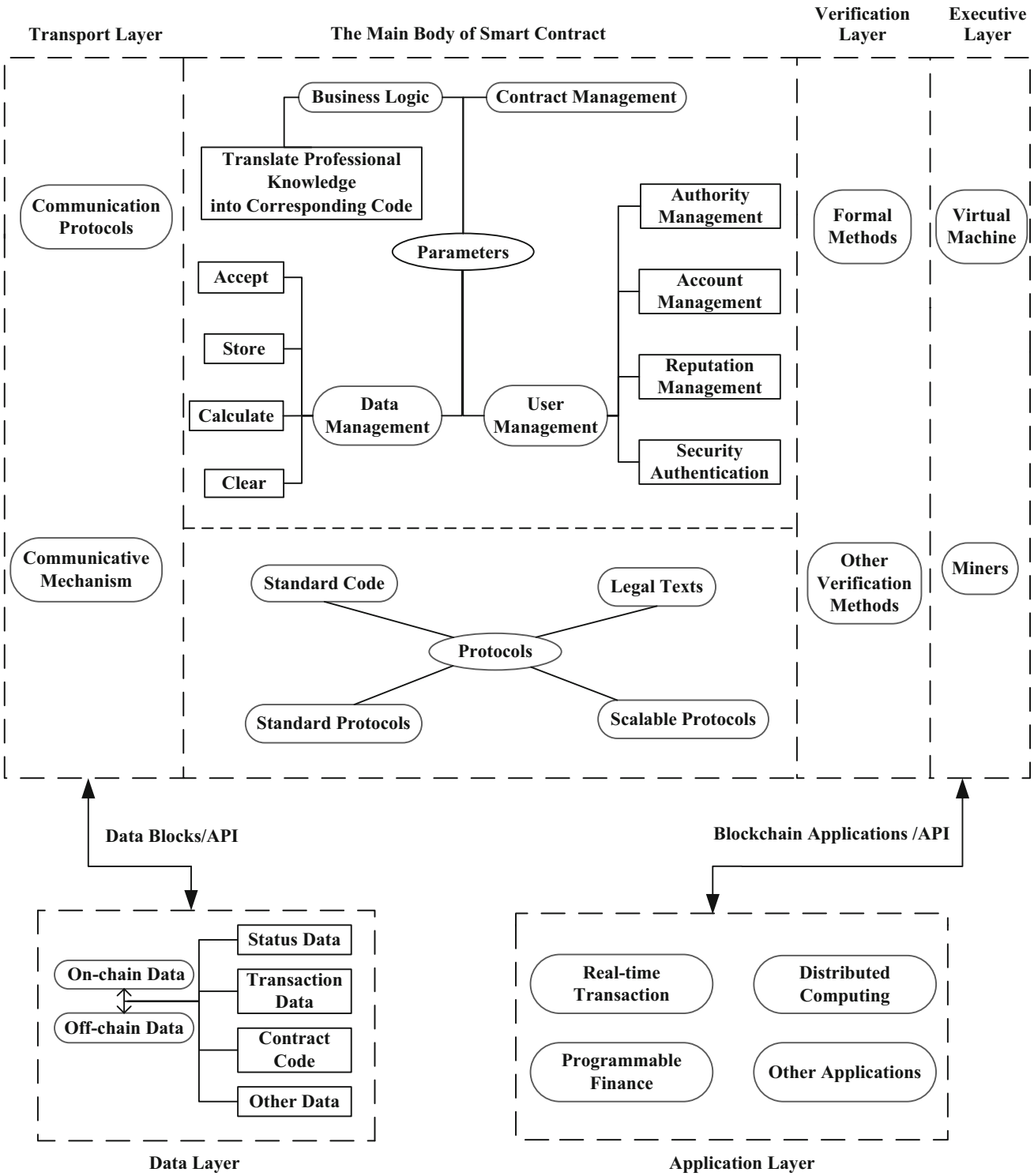


Fig. 3 The basic structure of smart contract

operation of it. The application-layer is an advanced application based on smart contract architecture, and it is mainly used to interact with computers, and then realize applications such as real-time transactions, distributed computing, programmable finance and others.

The biggest difference between smart contract and traditional contract is that smart contract uses the computer language instead of legal language to record terms [22]. To be more exact, smart contract is automatically executed by a computing system and is completely stored in the

computer. Smart contract based on blockchain technology has the characteristics of tamper proof and distributed transaction. Tamper proof is the most remarkable feature in the blockchain, and its specific performance in that once the smart contract is successfully deployed, then it cannot be changed. In addition, each executed contract can be synchronized to each user's data terminal due to the distributed feature. Smart contract digitally deploys the contract terms to the blockchain network in the form of code, and it will be executed automatically once the trigger conditions of the protocol set are met. The above features make smart contracts ideally applicable to the scenarios of contract terms, on account of it can reduce malicious tampering and human intervention [23].

Smart contracts have become a landmark product in the era of digital currency. With smart contract, not only people handle decentralized trading and manage digital assets, but also the court can use its characteristics to deal with various economic disputes. As a kind of computer technology, smart contract can not only process information effectively, but also ensure that both parties of the contract can perform the contract compulsorily without introducing the third-party authority, so as to avoid the occurrence of breach for contracts. That is to say, the implementation of smart contract can form consistent and non-controversial operation. It not only enriches the types of blockchain transactions, but also further expands the functions that is to meet the various needs of the digital economy. Although smart contracts have powerful functions, it also has some shortcomings. At present, the main risks faced by smart contract can be divided into three categories: privacy leakage, transaction overflow and exception, and denial of service attack, and smart contracts subject to these may never return to normal working state [24]. Hacker attacks have occurred many times due to the security of smart contracts. There are two typical cases: one is Bitfinex, a bitcoin exchange, was attacked by hackers, resulting in a loss of nearly $75 million [25]; another is the Dao event that hackers use reentry vulnerability to attack, not only caused a loss of more than 50 million US dollars, but also directly led to the permanent divergence of Ethereum [26]. As the increasing number of DApp, DApps running on ETH, EOS, TRON and others are constantly attacked by hackers. The main means of attacking DApps are as follows: transaction blocking, rollback transaction attack, false EOS attack, cracking random number, etc. In recent years, many security incidents also had taken place in the rapid development of the financial project with DeFi, and the main means of attack are as follows: liquid arbitrage attack on composable assets, pincer attack and Re-entrancy attack. Thus it can be seen that the security situation of smart contract is very serious. There are two main reasons why smart contract is easy to be targeted by attackers: one is that attacks on it have higher economic value, and the other is that contract loopholes will make contracts happen non-anticipatory action that results in it losing credibility. Therefore, with the increase of smart contracts and the large-scale development of blockchain in the future, the audit of contract code will become a specialized field of study [27].

The application of smart contract is still in the development stage at present, and mainly in the field of finance and government affairs. Smart contracts can help to achieve programmable currency and financial functions. Furthermore, smart contracts can improve the level and efficiency of automatic transaction, reduce the cost of transaction and execution, and facilitate the management of transaction action. Therefore, it has attracted the attention of financial institutions and central banks. Besides, smart contracts have widely application prospects such as digital payment, financial assets, cloud computing, IoT, sharing economy [28]. The value of blockchain does not lie in a single part, but in the interconnection and collaborative operation of different parts, and the smart contract can just play the central role. This means that a variety of practical functions can be realized on blockchain, which makes the current application system achieve unprecedented transparency and trust [29].

3 Basic knowledge of smart contract

Based on introducing the operating principle of smart contract, this chapter will further introduce the deployment of smart contract on Ethereum, Hyperledger Fabric and EOSIO platforms from the technical level, and make a comparative analysis of smart contract based on three development platforms.

3.1 Operation principle of smart contract

The system of smart contract automatically executes in the light of the trigger conditions contained in the information of event description, and the core of the whole system is that the smart contract is processed by the contract module in the form of transaction and event. When the transaction is successfully executed, the state machine of smart contract determines the state of contract. If all transactions in the contract are executed in sequence, the state machine will remove the contract from the latest block. Otherwise, it will continue to be saved in the latest block until the processing is completed. The whole process of transaction and state is automatically completed by the system of smart contract that built in the bottom of blockchain, and all processes are transparent and tamper proof. As shown in Fig. 4, the life cycle of smart contract [15, 28] is mainly

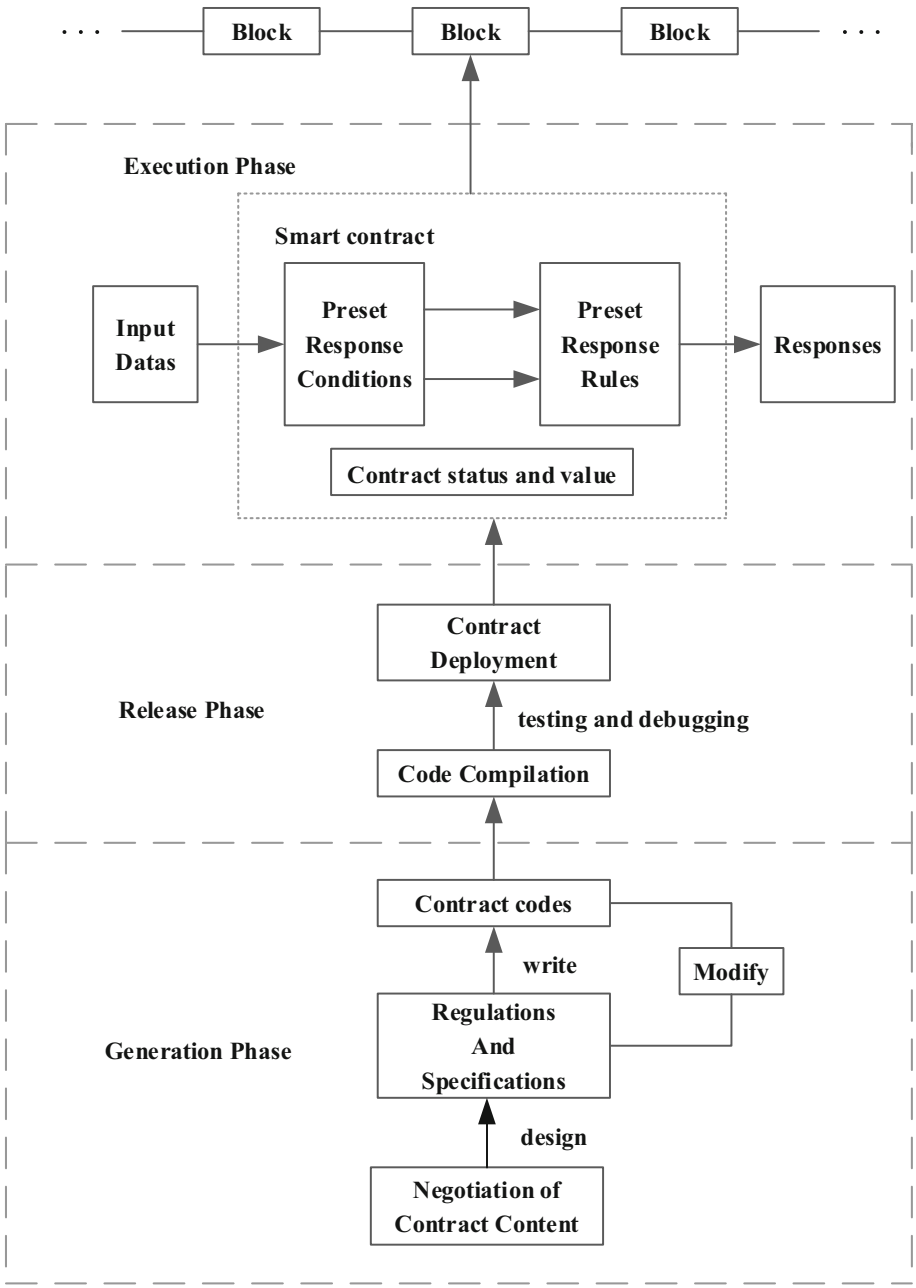


Fig. 4 The life cycle of smart contract

divided into three processes which generation, release and execution.

Each block in the blockchain structure of smart contract contains the following information: the hash value of the current block, the hash value of the previous block, the consensus timestamp, and other descriptive information [30].The operational principle of smart contract is shown in Fig. 5, which is mainly divided into three steps:

Step 1: multiple users participate in the formulation of smart contract, and the contract is programmed into code. Furthermore, the system of smart contract transmits the contract into the blockchain network after the participants sign with their private keys.

Step 2: the contract is spread to each node in the whole blockchain network through P2P. The specific process is that the verification node is responsible for storing and packaging the contract, and the contract is verified and will be finally written into the blockchain when the consensus is reached. Moreover, the main content of verification is whether the private key signature of participants matches the account.

Step 3: smart contract will check the state of the automaton regularly, and the transaction will be executed

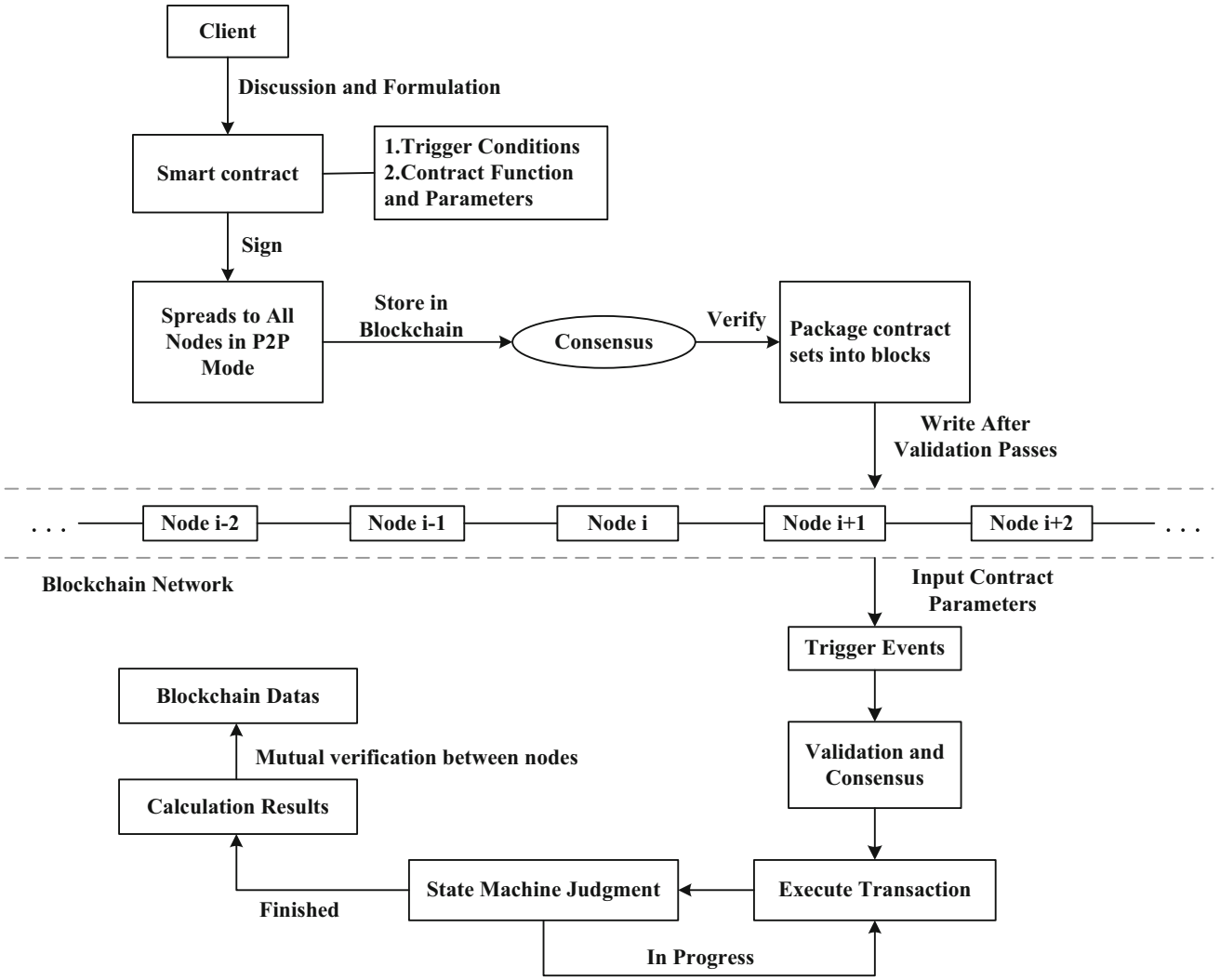


Fig. 5 The operational principle of smart contract

when the trigger conditions are met. In addition, the relevant blockchain data will be obtained if all the transactions in the contract are executed, or else the execution will continue until the completion.

3.2 Deployment of smart contract

Although the deployment of smart contract is compiled and executed on the graphical interface, the architecture and principle of its deployment are different when it runs on different platforms. This Section will introduce the deployment process of smart contract in different platforms from the technical level.

3.2.1 Ethereum

The deployment process of Ethereum smart contract is shown in Figs. 6 and 7 is an example of a trading smart contract code written using Solidity. It is needed to build appropriate development environment and download development tools before deploying smart contract. The development environment is mainly composed of EVM, Solidity and Geth. Ethereum Virtual Machine (EVM) is the running environment of smart contract, Solidity is the programming language of smart contract for EVM, and Geth (Go Ethereum) is the interactive command console [31]. And the development tools to be downloaded are shown in Table 1. In addition, since the deployment of smart contract on Ethereum mainly depends on the Ethereum node of Geth that running in the background, so that it is necessary to build an Ethereum network to run the node. The specific process is as follows: the Geth console uses the file that its name is genesis.json to create Genesis block, and it provides simultaneously the directory to save the block data and account private key. It initializes the network by executing commands, reading files and storing

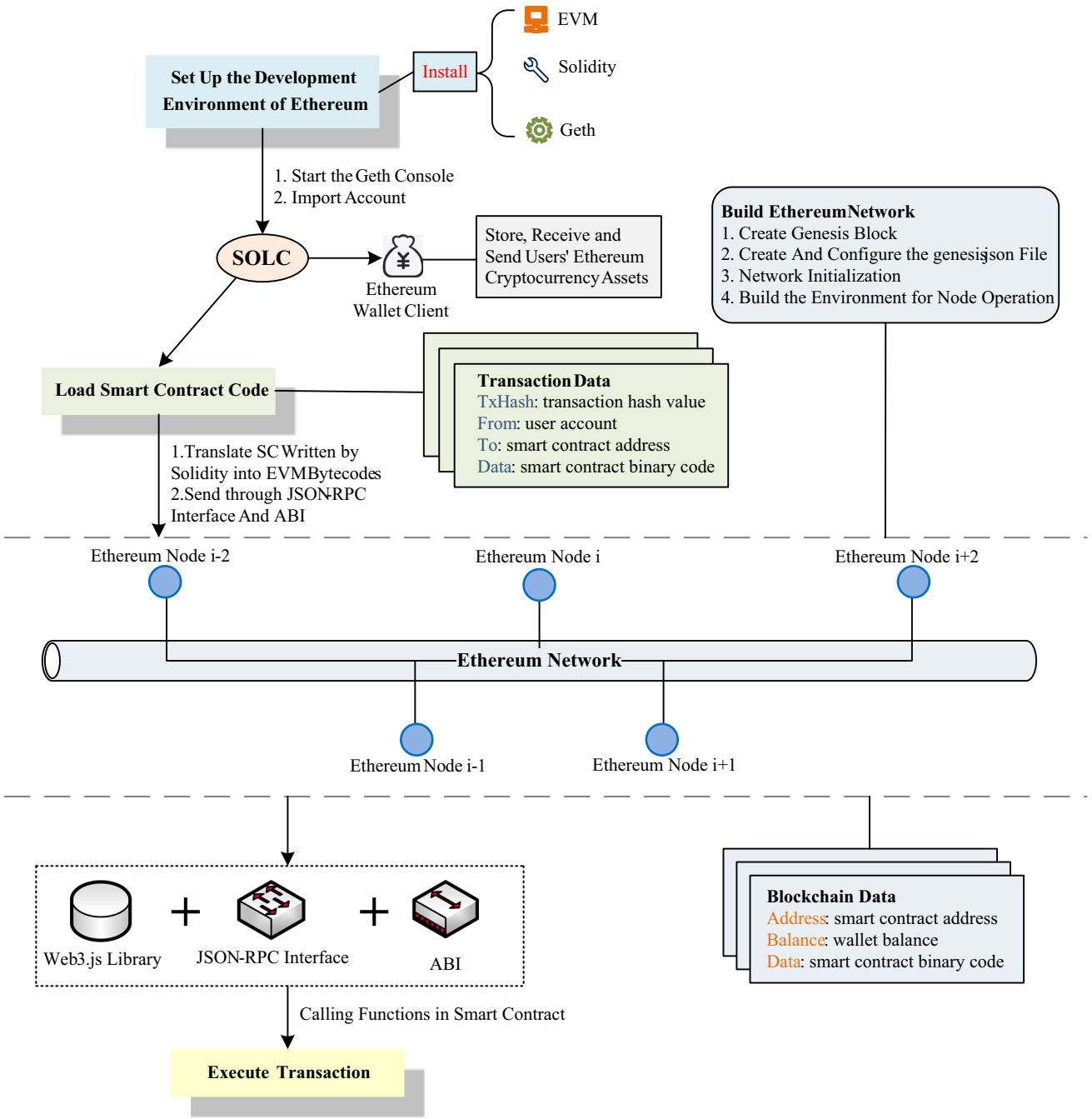


Fig. 6 Deployment process of Ethereum smart contract

block data, and configures relevant parameters to complete the construction of the node running environment.

Smart contract deploys bytecodes to Ethereum network through the transaction way, and a new smart contract account will be generated every time if it is successfully deployed. During deployment, the smart contract code written in the Solidity language is transformed into EVM bytecodes through smart contract compiler SOLC [32]. After that, smart contract is created through a transaction that contains key information such as the creator's account number, and the content and address of smart contract. It should be noted that the generation of smart contract address takes the creator's account number and the number of transactions sent as random number input, and creates a new address as the account number through the Kecca-256 encryption algorithm. Furthermore, it is needed to store data that contains binary codes of contract, address of smart contract and wallet balance in the blockchain.

```
pragma solidity >=0.4.22 <0.9.0;
contract OwnedToken {
    TokenCreator creator;
    address owner;
    bytes32 name;
    constructor(bytes32 _name) {
        owner = msg.sender;
        creator = TokenCreator(msg.sender);
        name = _name;
    }
    function changeName(bytes32 newName) public {
        if (msg.sender == address(creator))
            name = newName;
    }
    function transfer(address newOwner) public {
        if (msg.sender != owner) return;
        if (creator.isTokenTransferOK(owner, newOwner))
            owner = newOwner;
    }
}
```

Fig. 7 Solidity codes example of Ethereum smart contract

Table 1 Development tools of Ethereum

Tool	Function
Truffle framework	The popular Ethereum development framework. It has built-in functions that is smart contract compilation, link, deployment and others
Ganache	It can be used to create a blockchain network locally to test the program
Metamask	It is an Ethereum node wallet in the form of a Chrome plug-in
VS code and solidity plug-in	VS Code is a tool for writing Solidity code. It can be installed with the Solidity plug-in to support syntax highlighting
Remix	It is a smart contract development environment (IDE) based on Web browser

Ethereum provides a set of interface call based on JSON-RPC (Remote Procedure Call) [33]. In addition, through interface provided by Geth such as JSON-RPC and API (Application Binary Interface), the wallet client on EVM can also send the binary code of smart contract to Ethereum network, but the data transmission needs to meet JSON format. After the contract is deployed to the Ethereum network and the verification of the whole network nodes, the data will be written to each blockchain managed by Geth. And the functions in the smart contract are called through the Web3.js library and ABI interface to read and modify the data. Gas [34, 35] will be consumed as a service charge when testing and deploying DApp or smart contract on the actual Ethereum network. A certain amount of gas will be charged for each transaction on Ethereum, and the purpose is to confine that the workload required to execute the transaction, and pay for the execution. Due to the limited storage capacity of each block of Ethereum, swarm can be used as distributed storage to hash the stored content and generate proof of the blockchain.

3.2.2 Hyperledger fabric

The smart contract of Hyperledger Fabric is usually deployed in the form of chaincode. Chaincode is the carrier of business, and is mainly responsible for the specific business logic, in other words, encapsule the transaction definition and the processing logic into an interface. In addition, it can initialize and manage the ledger book status by applying the submitted transaction [36]. Chaincode is the middle point between the application layer and the bottom layer of blockchain, and the execution environment of each chaincode is a protected stand-alone container (Docker), which is isolated from the operation of endorsement node. Chaincode can be developed by the development language such as Go, Java and Node.js.

The deployment process of Hyperledger Fabric smart contract is shown in Figs. 8 and 9 is a java code example of the invoke method of chaincode. It is necessary to build the development environment of chaincode before deployment [37], that is to download Fabric components and the Docker images that are related to the chaincodes developed with Go or Java and node configuration. And the key components and corresponding functions of Fabric [38] are shown in Table 2. As a command-line tool, Docker Compose mainly implements batch processing in containers, which can help build Fabric networks. Fabric network is mainly built by generating the node certificate, creating the file of genesis block and the channel file, writing configuration files corresponding to Orderer nodes and Peer nodes. After setting up the development environment, it is required to install chaincodes on each peer node to execute transactions and endorsement transactions, and instantiate chaincodes on Channel. As an important part of Fabric, channel has the function of data isolation, and each channel can have an independent ledger and smart contract. The process of instantiating chaincodes on Channel is as follows: find the compressed package according to the parameter combination file name, compile the package after decompressed, generate the container and start it, and the peer node returns the processing results, submit the order and generate blocks. Init method, one of the methods that chaincode must implement, it needs to be called to perform initialization after chaincode finished deployment and received the transaction of instantiation or upgrade, so that chaincode can successfully perform the necessary initialization operations that includes initializing the application state. Each chaincode program must implement the chaincode interface, because the methods in the interface will be called when it responds to incoming

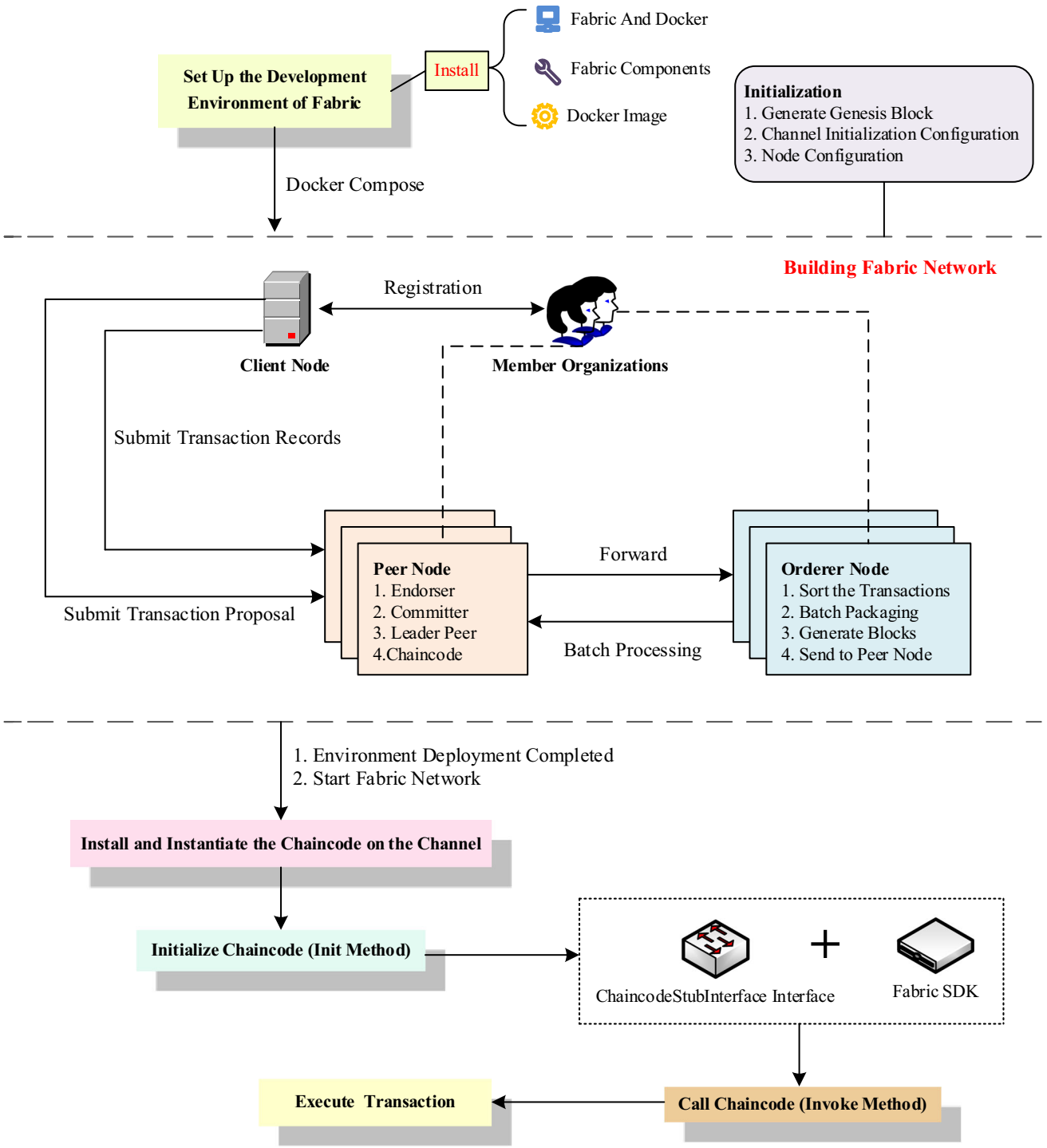


Fig. 8 Deployment process of Hyperledger Fabric smart contract

transactions. It should be recognized that the chaincode reads and modifies the account status through the methods provided by the API interface named ChaincodeStubInterface. The Fabric SDK can provide developers with a variety of ways to write applications to operate the blockchain network. Using the invoke method to call chaincode through the interface and SDK, and then execute the corresponding transaction.

3.2.3 EOSIO

EOS smart contract is a program registered on the EOSIO based blockchain and executed on the node, and it mainly

```
func (t *SimpleAsset) Invoke(stub shim.ChaincodeStubInterface) peer.Response {
    fn, args := stub.GetFunctionAndParameters()
    var result string
    var err error

    if fn == "set" {
        result, err = set(stub, args)
    } else {
        result, err = get(stub, args)
    }
    if err != nil {
        return shim.Error(err.Error())
    }
    // Return the result as success payload
    return shim.Success([]byte(result))
}
```

Fig. 9 Java codes example of invoking method of chaincode

realizes the specific function of contract and stores the request ledger of contract action in the blockchain. Each EOS smart contract has a set of operations and types, which *Action* represents a single operation, *Transaction* is a collection of one or more *Action*, and *Type* defines the required content and structure used in the contract. Furthermore, EOS smart contracts communicate with each other by the communication architecture based on messages and shared memory database, and it has two main interaction modes of it: Inline and Deferred [39]. The Inline mode mainly implements the real-time calling sequence of all actions in the transaction, while the Deferred mode mainly implements the delayed execution of some actions that are not executed immediately. EOSIO smart contracts are mostly developed in C++ language, executed by CPU, NET and RAM, and EOSIO based blockchain usually uses WebAssembly (WASM) that a new type of code to execute user developed applications or code [40]. More particularly, when the transaction of EOSIO based blockchain storage contract is in progress, the corresponding smart contract set must attached the Ricardian Contract [41].

The deployment process of EOSIO smart contract is shown in Figs. 10 and 11 is a C++ code example of EOS smart contract. EOS Studio is a graphical integrated development environment (IDE) for EOSIO DApp development, and Docker is the running environment of EOS smart contract [42]. The development environment needs to be built before deploying the EOS smart contract. Aside from downloading the main tools of EOSIO as shown in Table 3, it is also needed to install node.js package, EOSJS and scatter. EOSJS is a method library for interaction with EOSIO blockchain network, and scatter is a wallet front-end plug-in based on EOS. After that, it can start the Cleos command line to deploy the EOS smart contract after configuring the Docker Compose file. Firstly, it is required to load Eosio.bios, the basic IO smart contract. It is the basic system of many basic actions in EOS, and directly control the resource allocation and have access to API, thus it is necessary to ensure the effective execution of basic IO intelligent contract. On the public blockchain, Eosio.bios will manage the token that has raised and be raised to reserve bandwidth for CPU, memory and network activities. When the basic IO smart contract has finished loading, by signing the corresponding action of a function call in the smart contract through the private key of the account

Table 2 Key components of fabric

Key component	Function
Client	(1) Mainly responsible for interaction with the Fabric system
	(2) Implement management operations, such as starting and stopping nodes and configuring network
	(3) Implement the operation of chain code, that is install, instantiate and call the chain code
	(4) The common clients are the command client (CLI) and the application client developed by Fabric SDK
Peer	(1) It is a peer node in the decentralized network of blockchain, which is mainly divided Endorser and Committer by function
	(2) Endorser: it mainly checks, simulates and endorses the plan
	(3) Committer: it is mainly responsible for checking the transaction and legitimacy, and updating and maintaining the blockchain data and account status
CA (certificate authority)	(1) It is mainly responsible for providing identity information based on digital certificate to members of Fabric network
	(2) It can generate or cancel a member's identity certificate
	(3) Fabric can realize the management of permission control based on clear membership
Orderer	(1) It is mainly responsible for receiving and sorting the transactions of each node
	(2) In the case of concurrency, the transaction sequence of each node should be determined by Orderer nodes according to certain rules to reach a consensus, and the transaction should persist into the account book of the blockchain
	(3) Orderer nodes support multiple channels isolated from each other, so that transactions are only sent to related nodes, such as Peer nodes

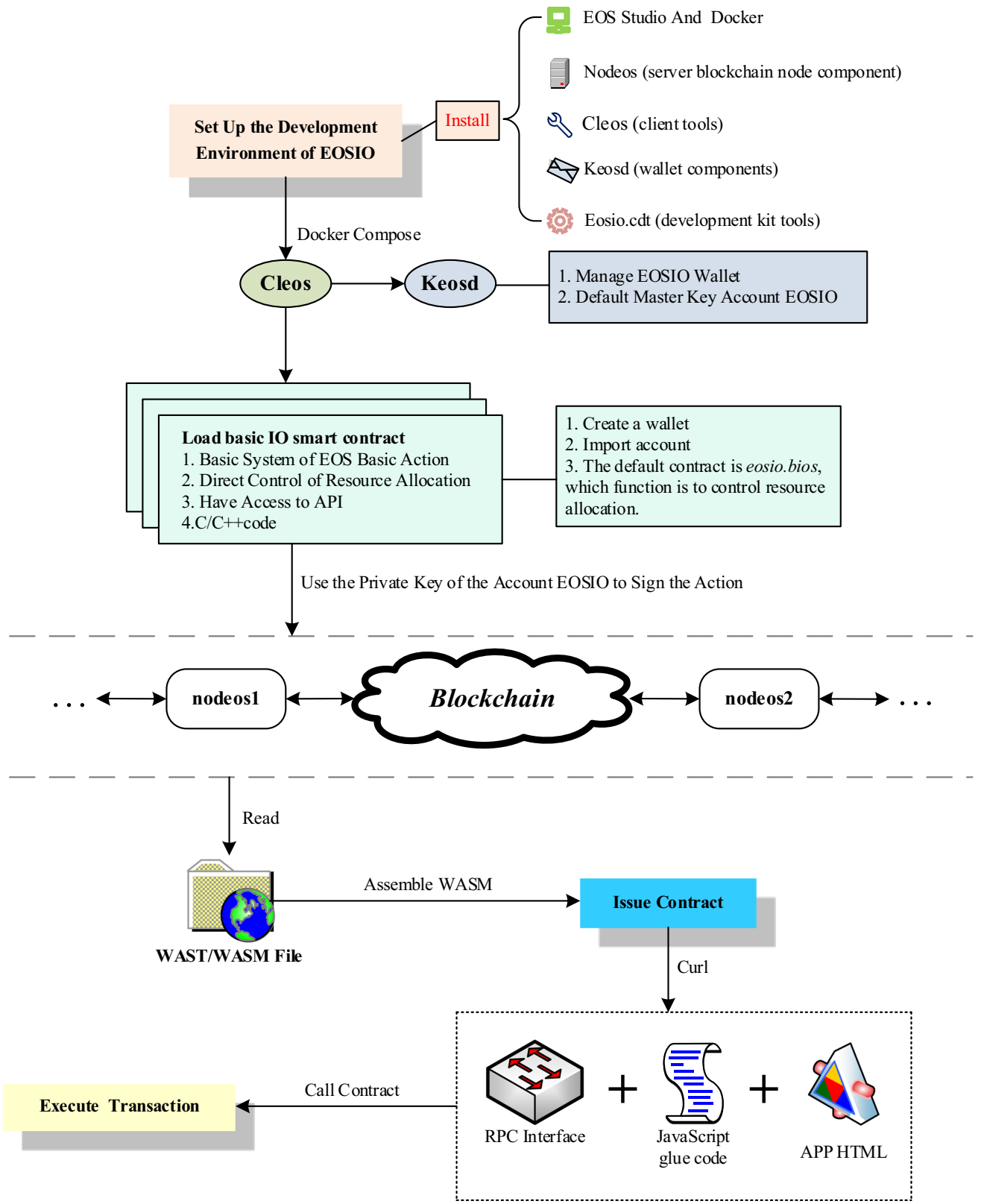


Fig. 10 Deployment process of EOSIO smart contract

```
#include <exchange.hpp>
using namespace eosio;
asset exchange::to_settlement_token(asset quantity, uint64_t price, bool floor) {
   //do many check
   uint64_t amt = quantity.amount * price;
   int64_t p = (int64_t)quantity.symbol.precision();
   int64_t p10 = 1;

   while(p > 0) {
      p10 *= 10; --p;
   }
   uint64_t res = amt / p10;
   if(!floor && res * p10 != amt)
      res++;
   return asset(res, settlement_token_symbol);
}
```

Fig. 11 C++ code example of EOS smart contract

Table 3 The main tools of EOSIO

Tool	Function
Nodeos (node + eos = nodeos)	(1) It is the core of EOSIO, and plug-ins can be configured to run the core EOSIO node daemons
	(2) Mainly responsible for the realization of core functions, such as data synchronization, the block generation, transaction verification, etc
Cleos (cli + eos = cleos)	(1) It is the client program of EOS and can interact with nodeos and keosd
	(2) It is mainly used to interact with blockchain and manage wallet
	(3) The command line tool that can upload the smart contract to the blockchain and can query the blockchain
Keosd (key + eos = keosd)	(1) It is mainly responsible for the related management of key, and stores the EOSIO key securely in wallet
	(2) Generating key pair, signing transaction, etc
Eosio.cdt	It is mainly used to generate ABI and convert C + + code into WASM text format

Eosio, the contract can be deployed to the Nodeos node. Finally, the EOSIO contract can be published after reading the WAST/WASM file and assembling the WASM. Smart contract only completes the core part of DApp that is transaction related operations, but most interactive interfaces still need JavaScript and HTML. In addition to using C++ or programming methods to call some RPC interfaces, the curl (a transfer tool) is the simplest way to call this interface. DApp can interact with other interfaces through RPC interface, and then achieve the goal that is to execute transaction by calling smart contract.

3.3 Comparative analysis of smart contracts based on three development platforms

Blockchain is a distributed system that can realize data cannot be tampered and trusted calculation results through multi-party storage and calculation [43]. And the smart contract must have two properties at the same time based on such characteristics: Certainty and Termination. The running results of different nodes may not be consistent if the smart contract with the uncertain, which will lead to the consensus not being reached and the network stagnates. Similarly, the node will spend infinite time and resources to run it if the smart contract is never stopped, and it will also lead to the stagnation of the network. Blockchain smart contract has strict requirements on the operating environment. The fundamental reason is that the current smart contract is running under the key that is Turing's completeness, and it must meet the requirements of certainty and termination [44].

The smart contract will run in multiple nodes of the blockchain network, and the detailed design of its specific development will be different in different operating environments. In Table 4, based on the three smart contract development platforms that is Ethereum, Hyperledger Fabric and EOSIO, we will compare and analyze them from the implementation details, such as the programming language, the consensus mechanism and the underlying database. Furthermore, we will also introduce the application environments of the smart contract based on different platforms. Moreover, we will also discuss the methods of solving the problems of two characteristics that are certainty and termination, and further summarizes the existing problems and corresponding solutions of the three development platforms [45–49].

4 DAG-based blockchain smart contract

As NXT community proposed to change the linked storage structure of blockchain into DAG (directed acyclic graph) blocks [50], researchers began to explore DAG technology [51]. At present, the most representative DAG-based blockchain projects mainly include IOTA, Byteball, Nano, HashGraph and InterValue, which adopts the concept of blockless and creatively use the data structure of DAG. However, it requires technological innovation to realize the smart contract function of DAG-based blockchain due to DAG does not take blocks as the underlying architecture [52]. The more mature projects in the development of smart contract are Hashgraph and InterValue. Byteball only supports simple declarative smart contracts that are not complete in Turing. IOTA also launched the Alpha version

Table 4 Comparative analysis of smart contracts based on three development platforms

Platform	Ethereum	Hyperledger fabric	EOSIO
Program language	Solidity	Golang/Java/Node.js	C++
Consensus mechanism	POW/POS	Solo/ Kafka/ Etcdraft	Graphene (DPOS + BTF)
Underlying database	LevelDB	NoSQL/LevelDB/CouchDB	Oracle, MySQL and other mainstream databases
Protocol	Ghost protocol/Whisper protocol	Gossip protocol	Bancor protocol
Core strengths	Support new development of rich ecosystem	Unique, highly elastic and scalable architecture	High performance and no handling charge
Operating environment	EVM (ethereum virtual machine)	Docker	Docker, building private network and connecting EOS community test network
Application scenarios	(1) It is the strongest public blockchain so far (2) Applications of Finance and financial derivatives, online voting, decentralized governance, identity authentication and reputation system, file storage, decentralized autonomous organization, supply-chain and insurance, etc	(1) It is mainly used in enterprise level licensing blockchain (2) Decentralized governance of smart contract, the new application mode of chain code for collaboration and consensus, private data security enhancement, external chain code initiator, improving state database cache for CouchDB performance and Alpine based the docker image, etc	(1) It is by far the most potential public blockchain (2) Set up wallets, gambling games, e-commerce, financial technology, markets, decentralized exchanges and content platforms on the public blockchain, etc
The methods to solve the problem of determinacy and termination	(1) Determinacy: to ensure the determinacy by EVM providing deterministic system functions and restricting the access types of data (2) Termination: fee meter solution and economic means to solve the problem of downtime	(1) Determinacy: try to avoid the use of non-deterministic functions when developing. And the platform plans to provide a set of deterministic system function library for users to use, and innovate in the accounting architecture (2) Termination: uses the timer scheme, but it will increase the failure rate of consensus algorithm	(1) Deterministic: adopting deterministic parallel technology. It is used to control the synchronization, competition and interference among the parallel program executors, so that the execution result of the program only depends on the input (2) Termination: uses the timer scheme
Existing problems at present	(1) Low throughput (2) Poor scalability (3) Security issues (4) High transaction costs	(1) High maintenance costs and delays (2) Low throughput and poor scalability (3) Security issues (4) Problems in cross channel smart contract call	(1) The ineffectiveness of supervision mechanism (2) The defects of economic model (3) Governance issues under consensus mechanism
The main ways to solve the problems	(1) The POS-Casper scheme of Ethereum (2) Sharding Technology (3) Channels, Mixers, Ring Signature, Zero Knowledge Proofs (4) Expansion	(1) Using IPFS as file transfer protocol (2) Identity confusion mechanism and PDC (private data collection) scheme (3) Data partition scheme of multichannel	(1) Imitating the stock model of Warren Berkshire (2) A new economic form (stacking) is put forward (3) The mixed mode of on Chain Governance and off chain governance

of IOTA smart contract protocol (ISCP) in 2021.In order to further explore the application value of DAG-based blockchain smart contract, this Section will introduce the basic knowledge of DAG-based blockchain and the deployment of smart contract for Byteball, InterValue and IOTA, and analyze the application advantages and disadvantages of DAG-based blockchain smart contract.

4.1 DAG-based blockchain basics

DAG-based blockchain takes DAG as its data structure and its network consists of transaction units, which can achieve asynchronous and concurrent write transactions, like multi-core and multi-threaded CPU [53]. Except the data structure is different from blockchain, there are also differences in granularity: each blockchain unit records multiple transactions of multiple users, and each DAG-based blockchain unit records single user transactions. It can be

Table 5 Comparative analysis of blockchain and DAG-based blockchain

	Blockchain	DAG-based blockchain		
		Byteball	InterValue	IOTA
Data structure	Information stored in blocks + Chain	Information stored in transaction units + DAG		
Communication mechanism	P2P technology	Web socket communication in json data format	Anonymous communication based on P2P + Tor + VPN	Asynchronous communication mechanism based on Gossip protocol and Tangle
Consensus mechanism	PoW, PoS, DPoS, PBFT, Raft, Ripple, etc	Mainchain and 12 notaries	Hashnet consensus based on enhanced DAG BA-VRF double layer consensus	Fast probabilistic consensus Cellular automata consensus PoW weight accumulation
Smart contract	EVM smart contract, Chaincode, EOSIO smart contract, etc	Declarative contract with non-Turing completeness (Smart Payments)	Declarative smart contract with non-Turing completeness and advanced Turing complete smart contract (MVM)	IOTA Smart Contract Protocol (ISCP)
Transaction cost	Need transaction fees	Need transaction fees	No transaction fees for local full nodes	No transaction fees
Double spending problem	UTXO and timestamp technology	Mainchain sequencing	Layering and sharding consensus mechanism + suffix matching method	Weight comparison of PoW
Transaction performance	The transaction speed decreases with the increase of nodes. Block competition. Not suitable for large-scale operation	No block limit. Transactions are carried out in parallel The time of each transaction decreases with the increase of nodes Able to maintain high transaction speed in large-scale operation		
Resource consumption	Reaching a consensus requires a huge consumption of resources	No block Simplified consensus Storage subsets can effectively reduce resource consumption		
Performance bottleneck	Poor scalability Throughput is limited by block size, network bandwidth and other factors	Good scalability The throughput increases with the increase of nodes, but is limited to network bandwidth and bookkeeper node performance		
Network security	Strong. Network security problems can be cause when the attacker has 51% of the computing power of the whole network	Stronger Network security is guaranteed by the randomness of transaction confirmation and expansion speed	The three development platforms have the same advantages in network security. Cells should be merged here.	
Application	It has a wide range of applications, mainly in the financial field, supply chain and Internet of things	Robot store, authentication, P2P insurance, market prediction, voting and IoT solutions	Digital currency, financial and non-financial applications. Practical technologies supporting large-scale applications are being explored	Focus on solving IoT transaction and data layer problems, such as automatic driving, smart flood protection, and supply chain

seen from the basic structure that DAG can achieve very high network scalability and throughput compared with the traditional blockchain technology. Through the comparative analysis of blockchain and DAG-based blockchain [51–54] in Table 5, the technologies adopted for different distributed models (such as IOTA, Byteball and InterValue) will be different, and the appropriate distributed model can be selected according to different application scenarios.

Through comparison, DAG-based blockchain has the following advantages over traditional blockchain:

1. Fast transaction speed: DAG can realize local processing and parallel computing, which greatly improves the transaction speed.
2. Strong scalability, high throughput and no capacity limit. With the increase in participants, the network also tends to be stable, and the transaction confirmation speed is faster and faster. There is no need to wait for data synchronization from other nodes. Therefore, DAG is very suitable for IoT projects.
3. Higher security: due to the data structure of DAG, if a node needs to be modified, the corresponding in-degree and out-degree also needs to be modified, making it more difficult to do evil.
4. Low cost: there is no block sizes problem due to no miners or blocks of DAG system, and users can execute transactions in very few currencies. Furthermore, DAG technology can process a large number of transactions in a few seconds, which is suitable for large transaction applications.

However, DAG-based blockchain also has some shortcomings:

1. Uncontrollable transaction duration: when verifying historical transactions in a random manner without any sequence rules, some transactions may not be verified by any other node in extreme cases, which resulting in that they will never be confirmed. This also led to the unpredictability of transaction duration.
2. Strong consistency is not supported: DAG asynchronous recording mechanism brings uncontrollable consistency problems while improves the scalability. As an asynchronous operation, DAG does not have a global sorting mechanism, which limits the types of operations supported by the system. What's more, it is likely that the data stored between nodes will deviate after running for a period of time when running a smart contract.
3. Security has not been verified by large-scale applications.
4. Large scale traceability is difficult: in order to track the relationship between each transaction and previous transactions, the whole DAG map needs to be retrieved and accessed at any time. In a large-scale system, the traceability of its transactions will be very complex, and it is almost impossible to save it all in memory for real-time update. If these data are saved from disk, refreshing the weight of each tangle in real time will cause a lot of random I/O, which may be solved by deploying a large number of SSDs (solid state disk).

The asynchronous communication mechanism of DAG-based blockchain has obvious advantages in improving scalability, shortening transaction confirmation time and reducing cost, but its security and consistency problems also need to be solved urgently. In the long run, DAG is a very novel and promising mechanism, which opens a new door for thinking in the field of traditional data management.

4.2 Byteball

Byteball adopts declarative smart contract with non-Turing completeness, which uses Boolean statements to write contract content, and supports Boolean operation and data storage [55]. It has the characteristics of simple deployment and high security. In addition, as the infrastructure of Smart Payments [56], Byteball smart contract can call Byteball wallet to pay transaction fees. Byteball is different from other DAGs in that it implements make use of Oracle to solve the problem of transaction order. The role of Oracle is to track the execution of all transactions and maintain the global order for all transactions in the network [57]. In this way, by using Oracle, smart contracts that require accurate transaction execution order can be realized.

Byteball smart contract mainly realizes the transaction payment function. Its formulation and deployment are very friendly and readable for users. Taking the test network as an example, we introduce the deployment process of Byteball smart contract, including the following steps:

Step 1: installs and starts the Byteball wallet, and request token (bytes) by sending the payment addresses to the test network Faucet.
Step 2: In essence, the formulation process of Byteball smart contract is similar to user interaction in the chat interface. User need to add transactions to their address book and establish interaction channels, which is the biggest difference in traditional blockchain deployment and the key step of contract formulation.
Step 3: Both parties send payment addresses to each other through the chat function provided by Byteball wallet. In order to ensure privacy, the original address needs to be hashed and use base32 coding algorithm to obtain the payment address. When sending the data unit (Unit) with the payment address for the first time, the user needs to put the corresponding address definition into the authors field of the Unit.
Step 4: Both parties use addresses to define contract content, which is presented in the form of Boolean logic. The simplicity of this logic is conducive to checking logic vulnerabilities and reducing the risk of security vulnerabilities in the process of writing contracts. Binding the events in the physical world to the payment conditions through the third-party Oracle, and the events are introduced into the payment execution conditions of the smart contract as a data feed. After the contract

```
["or", [
    [ "and", [
        ["address", "ADDRESS Alice"],
        ["in data feed", [ [ "EXCHANGE ADDRESS" ] , "USDCNY", ">", "1.888"] ]
    ] ],
    [ "and", [
        ["address", "ADDRESS Bob"],
        ["in data feed", [ [ "TIMESTAMPER ADDRESS"], "datatime", ">", "2021-08-25 00:00:00"]]
    ]]
]]
```

Fig. 12 Code example of using payment address to define smart contract in Byteball

content is formulated, it will be sent to Byteball consensus network, and the witness will verify and confirm the contract content.

Step 5: Byteball can realize rich payment logic on the payment address. The user sends a payment request in the form of a complete Boolean statement of the smart contract to the transaction party, and the authenticators field will verify the validity of the unit. After the Unit verification is passed, if both parties of the transaction made payment and received confirmation information of payment, then the execution of smart contract is completed.

In order to better understand the simplicity brought by the Boolean logic of Byteball smart contract, a code example of defining smart contract using the payment address is given as shown in Fig. 12. Alice and Bob respectively transfer bytes to the gambling payment address generated by the above definition, and sign the generated data unit. When the exchange rate published by the exchange exceeds 1.888, Alice has the right to dispose of all assets on the gambling payment address. If it does not exceed 1.888 before August 25, 2021, all asset disposal rights belong to Bob. If both conditions are met, Alice and Bob have the right to dispose.

The Boolean logic syntax of Byteball smart contract makes the contract highly readable and concise, and reduces the risk of contract vulnerabilities. However, the function is relatively single, which is weaker than the traditional blockchain smart contract function in terms of completeness. However, because the unique function of Byteball is its built-in secret asset (Blackbyte) and its positioning is to become the ledger of the IoT, the efficiency and privacy in the transaction payment are the development focus of Byteball smart contract.

4.3 InterValue

InterValue mainly solves the three problems of the existing public blockchain (low performance, high development threshold and low security). It uses the combination of Hashnet [58, 59] consensus based on DAG and Byzantine negotiation based on random selection function (BA-VRF) [60, 61] to realize million level TPS, which has the characteristics of anti-quantum attack [62–64] (using NTRU-sign-251 signature algorithm [65]). Security is improved through the bottom P2P anonymous communication network and the upper anonymous transaction method, and the high-performance smart contract is realized by Moses virtual machine (MVM). The difference between InterValue and other DAGs is that it adopts the DAG ledger (Hashnet) of Lattice structure [66], which each lattice in the ledger represents a local full node bookkeeping structure.

InterValue adopts hierarchical thoughts similar to computer storage architecture in the realization of smart contract function, and supports declarative smart contract with non-Turing completeness and advanced Turing complete smart contract. MVM is mainly used to execute these two smart contracts. However, because the declarative smart contract with non-Turing completeness is embedded in the transaction data unit in JSON data format, MVM cannot execute it directly. The main solution is that the local full nodes provide the compiler function of declarative contract language, so that the contract content can be compiled into the default contract object, and then executed by MVM. More particularly, the transaction handling fee is calculated according to the bytes occupied by the contract. The deployment process of declarative smart contract with non-Turing completeness on InterValue is the same as that of Byteball smart contract, so we will not be repeated here. Next, we will mainly introduce InterValue advanced Turing complete smart contract.

The advanced Turing complete smart contract for InterValue is mainly used to develop DApp with more complex program logic, but its deployment of is relatively difficult and is still in the continuous improvement stage. In order to realize the function of Turing's complete smart contract, InterValue adopts double-layer consensus structure and ex post rollback mechanism [67] to cancel the illegal output state of smart contract, which avoids the occurrence of double spending transaction. In addition, for reducing the development threshold, InterValue uses the independently developed Moses high-level programming language to write smart contracts, and supports the secure access and use of off-chain data. Advanced Turing

complete smart contract is verified and executed in MVM. Furthermore, MVM adopts the principle of stack-based virtual machines, which is simple and easy to use, and can provide portability of virtual machines. In terms of security, MVM adopts the sandbox structure design based on white list to protect the smart contract for malicious attacks of the system layer.

The advanced Turing complete smart contract is compiled into bytecode by Moses compiler and deployed to the InterValue network in the form of transaction data unit. MVM loads data such as variables and methods of smart contract in the method area. After the smart contract is instantiated, the heap of the virtual machine will allocate storage space for the instance object of the smart contract. When the smart contract is called and executed, MVM creates a virtual machine stack in the instruction scheduling area, which is mainly used to handle the stack in and out of the stack frame during the calling and completion of the contract method. At this point, the program counter will store the address of the next bytecode instruction to be executed. Since the smart contract takes the INVE Token consumed by the program running as the handling fee, a certain amount of INVE Token needs to be frozen when the user invokes the contract. With the execution of the instruction, tokens are gradually consumed until the contract is executed, and the remaining tokens will be returned to the user. If all tokens are consumed before completion of execution, contract status will be rolled back to the status before execution, and the consumed tokens will not be returned. This anti-fraud mechanism can reduce the damage to its network performance by attackers using contract vulnerabilities.

Compared with blockchain smart contract, the main advantage of InterValue is that it provides advanced smart contracts for off-chain data access. In terms of design, InterValue integrates UTXO and account transaction. For the sake of ensuring security and execution efficiency, the smart contract for InterValue has made a breakthrough in secure access and use of off-chain data, enhanced the security of the virtual machine itself, and realized the embedded formal verification of smart contract code. InterValue still has great potential for realizing highly practical distributed application development in the future. However, the implementation of Turing complete smart contract with DAG still faces some challenges, such as establishing the model of account state, how to store the data of account state in the network, and storage in the process of state change.

4.4 IOTA

As one of the representatives of blockchain 3.0, IOTA aims at design a new transaction settlement and data asset circulation system for the IoT industry and provide scalable solutions by achieving data integrity in the economy between machines [68]. Different from other DAG-based blockchain, it is a DAG-based blockchain based on Tangle [69], in which the connected nodes are transaction data, and consensus is an inherent part of the system. It can overcome the inefficiency of the blockchain and has the characteristics of zero transmission cost, unlimited expansion and data security. Moreover, Tangle is the core technology of IOTA, which has the characteristics of no miner, relatively loose data transmission rules and scalable data units. In IOTA, Markov chain Monte Carlo algorithm (MCMC) [70] is used to solve the problem of selecting attachment points in Tangle. In order to deal with conflicting transactions in Tangle, Coordicide proposed fast probabilistic consensus (FPC) [71] and cellular automata consensus (CC) [72]. IOTA own mechanism can prevent heavyweight attacks [73, 74], parasitic chain attacks [75], splitting attacks [76] and quantum computing attacks.

Early IOTA did not have the function of smart contract, and Qubic project is committed to the implementation of IOTA smart contract. IOTA smart contract protocol (ISCP) was officially launched in 2021 and is currently in Alpha stage. ISCP Alpha is based on Rust and Webassembly framework, verified by Tangle, and runs in a multi chain environment protected by Tangle. In particular, the verifier does not need to verify all chains at one-time, because the creator of ISCP can choose a verification committee that matches its required or desired level of dispersion and security.

ISCP is defined as an immutable state machine: each smart contract has a state attached to Tangle. This status includes data such as account balance, input conditions and results over time, and each state update represents a state transition on the Tangle. The state and smart contract program code are immutable because they are stored on the Tangle. But it can incrementally update the state by attaching a new transaction to the Tangle state. Tangle provides verifiable audit trail of state transition. Therefore, it will not be destroyed by malicious nodes when state transition. The deployment process of ISCP based on the Goshimmer test network is shown in Figs. 13 and 14 is a code example of ISCP for verifying access rights (from GitHub). Before deployment, it is necessary to build the Rust development environment for ISCP, download main development tools of ISCP and docker images related to Go language. Development tools and corresponding functions required by ISCP are shown in Table 6. First, it needs to use the Coordicide solution, use Bazel to build the Tangle network, and run it through Docker. The smart contract written in Go language is programmed into binary bytecode through Rust Compiler, and the trading assets are delivered through Trinity wallet. Solo uses Go and GCC to

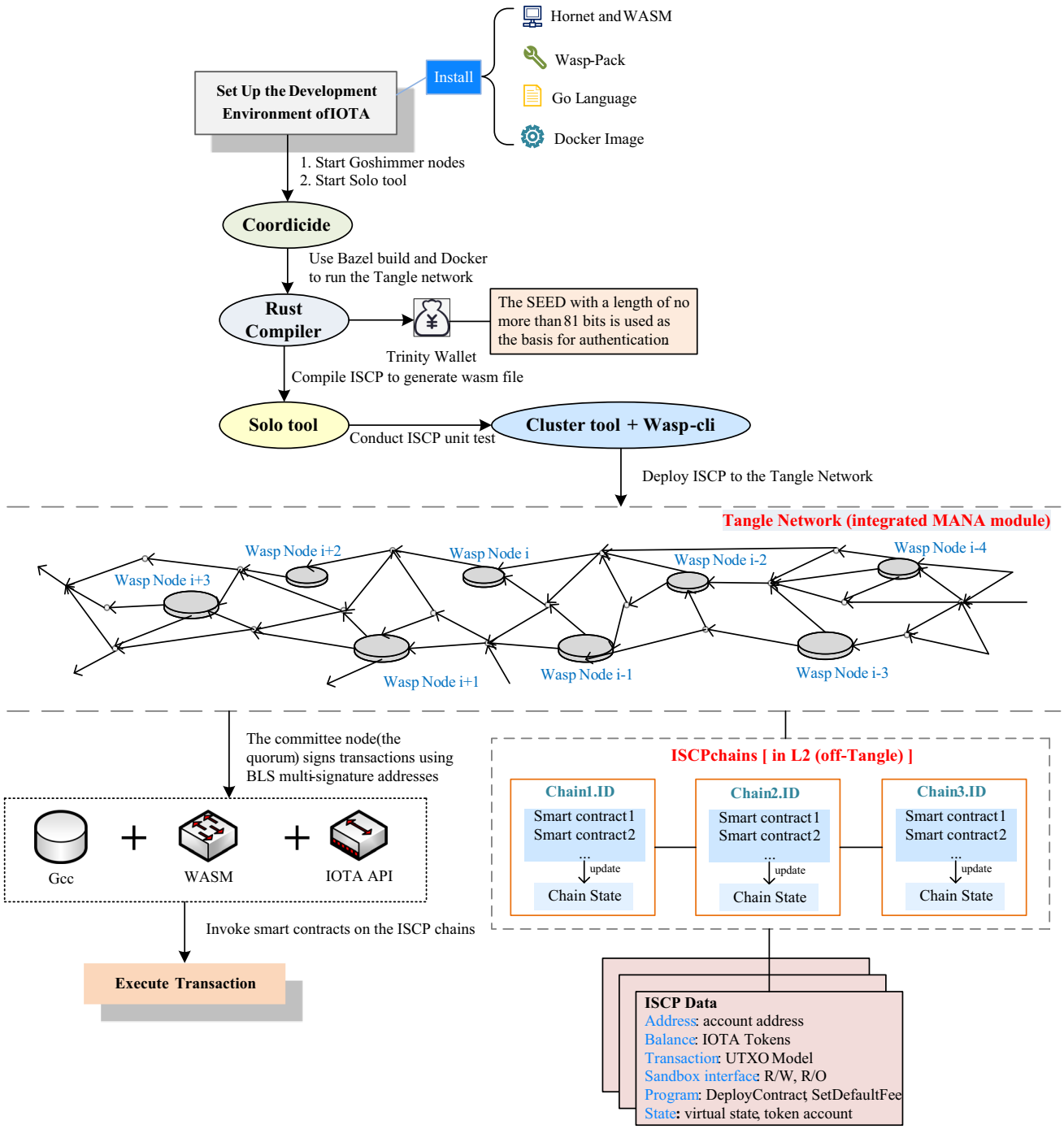


Fig. 13 Deployment process of ISCP

simulate the behavior of Wasp nodes, which can realize the unit test of smart contract. After the test is completed, the deployment of smart contract for Tangle network is realized through the Cluster Tool and Wasp command line. The smart contract chain run by Wasp node signs the transactions in the smart contract when the Committee node reaches a consensus result with result essence hash, a set of partial BLS signatures and a timestamp. Through WASM and IOTA API, methods within smart contracts can be called to execute transactions. It should be noted that the smart contract program uses the request transaction and the current state transaction to build the state update chain triggered by the incoming request, and stores the program hash in the Tangle to ensure invariance.

The smart contract function of ISCP is similar to the smart contract for Ethereum. However, due to the

```
fn my_iota_sc_function(ctx : &ScFuncContext){
    /// Panics if caller is not the contract creator
    access::caller_must_be_contract_creator(ctx);

    /// Panics if caller is not the chain owner
    access::caller_must_be_chain_owner(ctx);

    /// Panics if caller is not the contract itself
    access::caller_must_be_contract_itself(ctx);
}
```

Fig. 14 Code example for ISCP to verify access rights

Table 6 Development tool of ISCP Alpha

Tool	Function
Rust environment	It is used to write smart contracts and compile them into WebAssembly (wasm) binaries to prepare for the deployment of smart contracts on the chain
Cluster tool	It allows to use a Goshimmer (with simulated token ledger) and many Wasp nodes to run an isolated test network, which is mainly used to deploy chains and smart contracts, support DApp front-end to run, and run integration test
Solo tool	Write unit tests for smart contracts and DApps
Wasp-cli	A command line interface for interacting with wasp nodes. When deploying chain and smart contracts, tokens can be used for payment through addresses and accounts on the chain
Wasp explorer	A simple dashboard through which anyone can view information such as node configuration, deployed chains, smart contracts and accounts on the chain
IOTA API	It can be called through Curl, Python, JavaScript and Java

characteristics of Tangle structure, ISCP has high flexibility and faces some challenges:

1. State bifurcation: the state is updated in different ways when two or more transactions are attached to the Tangle, which results in the problem of conflicting copies. The current solution is to create a unique coin-mixing [77] when setting the smart contract, and embed the dye coin to the smart contract address, so as to form a non forkable chain during the transaction and prevent the occurrence of state forking.
2. Development environment upgrades: the verifiability and auditability of smart contract still needs to be further developed. Moreover, ISCP needs to realize binary compatibility with Ethereum ecosystem, and use Solidity as contract programming language. In addition, it is also necessary to implement the inter chains atomic exchange framework of local and external blockchain.
3. Security: it is necessary to ensure the independence of grass-roots snapshots and expand the unlicensed chain committee venue. Keys also need to be managed for security and scalability.

Although ISCP started late, its flexibility can provide scalable solutions for IoT. At present, it is still in the continuous testing stage, and the performance and advantages in large-scale applications still needed to be studied. DAG-based blockchain has great application potential for the scalability development of industrial Internet, but DAG-based smart contract is still in a state of continuous development, with higher flexibility than blockchain smart contract, but poor security and functionality. How to integrate smart contract engine into DAG system to realize the functions of big data security, privacy computing, automation and high transaction efficiency is a research hotspot in the future.

5 Research on the application status of smart contract

Blockchain is in the stage of 2.0 at present, which smart contract based on blockchain is widely used in real life for its decentralization, transparency and tamper resistance. Therefore, this chapter will further discuss the research status of blockchain smart contract, and introduce the current application status of it from mainly seven aspects: financial transaction, Internet of things, medical application, supply chain, EOS application research, Blockchain Oracle and other applications. In addition, in Sect. 6, we will further discuss the application research status of blockchain smart contract in industrial scale and the potential for large-scale application in the future.

5.1 Relative application and research of smart contract based blockchain

The latest report from PwC (Pricewaterhouse Coopers) shows that 2025 will be a turning point if blockchain technology is applied largely across the world. In addition, the application of blockchain will bring a growth of US $1.76 trillion to global GDP (1.4% of global GDP) by 2030 [78]. It follows that blockchain can not only promote the development of scientific and technological innovation, but also drive the world economy. Countries all over the world have formulated the overall development strategy of the blockchain industry, and blockchain technology seems to have become the next competitive place. As the blockchain further becomes a new infrastructure for the development of digital economy, it will lead a new round of global technological innovation. Major developed countries in the world will pay more attention to blockchain technology, which will increase industrial support for it and enhance

Table 7 Major international blockchain smart contract projects

Project name	Research team	Brief introduction
Ethereum	ETH Team	1. General development platform for smart contract 2. High contract liquidity 3. Higher security and transaction efficiency 4. Decentralization, automation, tamper-proof, transparency, etc
Hyperledger	IBM and Linux Foundation	1. A globally deployable, scalable and powerful smart contract development platform 2. Enterprise consortium blockchain 3. It can carry out complex calculation 4. Have pluggable modules
EOSIO	Block.one	1. Realizing the function expands of distributed application 2. No charge 3. Deal with larger TPS 4. Parallel execution of smart contracts
Polkadot	Web3 Foundation	1. Scalable heterogeneous multi chain technology 2. The contract module supports WASM smart contract 3. Adopt Polkadot Substrate development framework 4. Promote the development of cross chain interoperability
ChainX	PolkaX	1. The first ecological chain based on Polkadot technology framework 2. The core is to make the parallel chain of smart contracts 3. Contract module integrated with Substrate 4. Good usability, low cost and high automation
Certik	Certik Team	1. "Deep specification" formal verification technology provides code security audit services for smart contracts 2. Based on smart-tag and hierarchical decomposition technology 3. Improve the flexibility and efficiency of security verification 4. High scalability and automation
pLIBRA	LibraChina Team	1. Connect Libra blockchain to Polkadot for smart privacy contract of cross-chain interaction 2. Privacy protection through TEE technology 3. Based on Phala Network, being committed to the privacy protection of smart contract in Web3.0 ecology
ANTCHAIN	Blockchain Team (ANT Group)	1. The world's first commercially available On-chain privacy protection technology 2. Smart contract of hardware TEE privacy chain based on Intel SGX technology 3. Customized hardware processor of blockchain smart contract
Matic	Matic Team	1. Matic Network is the smart contract development solution of Ethereum Layer2 2.Adopt the frame of "Hybrid POS + Plasma Side-chain", with high throughput 3.Using the side-chain to trade and expand of off-chain
RSK/ RootStock	RSK Labs	1. The first open-source smart contract platform that has used the side chain with bitcoin bi-directional anchored 2. It has Bitcoin-level security and Ethereum-level flexibility 3. RIF OS framework and merged-mining algorithm are adopted 4. RVM is highly compatible with EVM at bytecode level
XuperChain	Baidu XuperChain Team	1. Blockchain 3.0 solution with strong network throughput and high concurrency of general smart contract processing capability 2. Supporting parallel chain and side chain 3. The original XuperModel data model is used to maximize the parallel execution capability

Table 7 (continued)

Project name	Research team	Brief introduction
LiquidApps	Liquidapps Team	1. EOS Network expansion solution 2. Build DApp Network and externalize CPU and RAM from EOS blockchain to reduce the difficulty and cost of development 3. Based on EOSIO side chain, its smart contract can access data without trust in a personalized way
AnnChain	AnnChain Team	1. One of the two open-source community projects of DApp Ledger of MIIT 2. Support "EVM + JVM" smart contract execution mode 3. two sub-projects: Annchain.Genesis and Annchain.OG 4. Solve the balance of scalability, decentralization and security

national competitiveness in blockchain technology and industry. This Section will introduce the current research status of international blockchain projects, and further explore the application and development trend of smart contract.

5.1.1 Research on relevant application in the world

Blockchain is changing the application scenarios and operation rules of many industries with its unique constructing mechanism of trust along with the evolution of it from 1.0 to 3.0 era, which is one of the indispensable technologies for the future development of digital economy and the construction of new trust-system. Foreign giants such as Google, Microsoft, JPMorgan Chase, Facebook, Amazon and IBM have started to study blockchain technology, and launched technical solutions and applications [79]. Moreover, international open-source organizations such as Ethereum foundation and Hyperledger community vigorously promote the innovative development of blockchain technology, which will effectively promote the iterative development of it. Ecosystem of blockchain covers all aspects of the global economy and society, which blockchain technology has seen an explosive development, and has carried out a series of applications in the fields, such as financial services, supply chain management, intelligent manufacturing, social welfare and health care [80, 81].

Up till now, besides 22 national governments and 73 international organizations have paid public attention to the development of blockchain platform software, there are 289,200 global start-up projects and 9635 patents have been published, in which America (29%) and China (18%) are considered to the most advanced in the development of global blockchain technology. Besides, typical of foreign companies including IBM, Alibaba, Oracle, Mastercard, Microsoft, Amazon, Cosmos, IOTA, EOS, Ripple, Stellar and MOAC. The main international blockchain smart contract projects now are shown in Table 7.

The application advantages of each blockchain smart contract project are as follows:

1. Ethereum project has the characteristics of decentralization and high efficiency of contract formulation. It does not rely on the participation of third-party authoritative institutions or central institutions. It can complete the transaction only through smart contracts, greatly reducing the intermediate links of protocol formulation, improving the efficiency of protocol formulation, and is widely used in many professional fields.
2. The design principle of Hyperledger Project is to develop a globally deployable, scalable and powerful blockchain platform that is focusing on privacy and future auditability. Hyperledger Fabric is an excellent representative of Hyperledger project. Fabric uses Docker technology to package smart contracts called chaincodes and it can run the components of smart contracts in isolation from other processes. Additionally, it has the characteristics of complex computing, pluggable modules (for enterprise customization and expansion) and high recognition of enterprise consortium blockchain.
3. EOSIO architecture provides the account, authentication, database and asynchronous communication, as well as application scheduling across multiple CPU cores or clusters, which aiming at achieving the vertical and horizontal expansion of DApp. Moreover, EOS smart contract has the advantages of no service charge, high throughput, better scalability potential and high performance. And EOSIO has the function of asynchronous parallel execution of smart contract, which can be better applied to projects with large amount of data and easy network congestion.
4. Polkadot project consists of many Parachains with potential differentiation characteristics. Furthermore,

the smart contract platform in Polkadot ecology is mainly based on WASM virtual machine, and using ink, an embedded domain specific language based on Rust language, which can promote the development of real cross chain interoperability.

5. As an ecological project of Polkadot, ChainX is the parachains and cross-chain asset gateway of Polkadot, and is gradually evolving into the secondary relay chain of Polkadot. Currently, ChainX has released the world's first smart contract platform of Bitcoin. Being a new starting point, ChainX 2.0 updates all codes to Substrate 2.0, and improves performance through the consensus upgrade, on-chain governance, off-chain workers, multi signature and other optimization methods. In the future, it can truly achieve the application development of Bitcoin cross-chain smart contract.
6. Certik a distributed application project that uses mathematical methods (formal proof) to check the vulnerability of smart contracts, and it has three advantages as follows: firstly, it has a mature formal verification framework and a complete theoretical basis; secondly, the complex smart contract can be subdivided into different modules for distributed verification based on smart tag and hierarchical decomposition technology, which greatly improves the flexibility and efficiency of security verification and has high scalability; thirdly, it is to complete contract verification automatically through the verification engine and audit algorithm, which has a high degree of automation. Furthermore, Certik AutoScan Engine (case), the first generation of high-performance automatic detection engine for smart contracts, has been released at present, which further promotes the development of smart contracts security.
7. pLIBRA is a Web3 foundation project (Grant Plan). It is developed based on the framework of Substrate, and the main highlight is the smart privacy contract that connects Libra blockchain to Polkadot for cross-chain interaction, which can realize the security of cross-chain interaction and sharing of smart contract. As a representative application of Phala.Network, pLIBRA is a confidential smart contract platform based on Trusted Computing Technology (TEE), and its goal is to provide enterprises and users with the infrastructure of confidential computing and data protection.
8. ANTCHAIN has the world's first commercially available on-chain privacy protection technology. Its core technology includes data encryption transmission protocol, data encryption storage protocol, remote authentication and key agreement protocol and a smart contract engine based on TEE. The platform provides a stable, efficient and secure execution environment of Turing-complete smart contract. At present, a customized hardware processor, ANTCHAIN All-in-one Machine, has been developed for blockchain smart contract.
9. The biggest feature of the Matic project is Matic Network. Matic Network is the only blockchain project supported and incubated by Coinbase and Binance. It carries out off-chain transactions and smart contract expansion through the side chain, in which the solution of smart contract expansion is realized by using the side chain supported by the security of Plasma framework, and without high transaction costs. Besides, Matic adopts a truly decentralized mechanism, and uses its own technology and highly autonomous ecology to create a Layer2 solution to adapt to the upgrade of Ethereum.
10. The technical definition of RSK is a side chain of bitcoin, which uses to continue the ecology of bitcoin. RVM, the virtual machine of RSK, has Turing completeness of smart contract, which is highly compatible with Ethereum's EVM, so that Ethereum DApp can seamlessly switch to the smart contract platform of RSK. Moreover, RSK using the double token mechanism of RIF and RBTC to pay the service charge can make the deployment cost of smart contract lower and the efficiency higher. And the operating system RIF OS developed by RIF laboratory can better meet the needs of the future development of Bitcoin ecology.
11. XuperChain is a high-performance, high concurrency blockchain 3.0 solution independently developed by Baidu. It has four core technologies: in-chain parallel technology, pluggable consensus mechanism, the permission system of account and integrated smart contract. Among them, in the aspect of smart contract, XuperModel, the original data model, is used to maximize the contract parallel execution ability, from this can support contract resource audit and shield the operating system interface to ensure security. At the same time, it can extend the multi development language of contracts and the access ability of resources on the chain to achieve scalability, and has the isolation property that different contract calls do not affect each other.
12. Liquidapps is committed to developing a side chain (DApp Network) based on EOSIO. Its R & D achievements such as LiquidAccounts Service, LiquidOracles and Zeus development kit can make the development of smart contract and DApp more simple and low cost, with the characteristics of easy use and strong scalability. Additionally, vRAM, the

proposed storage solution by Liquidapps, has the advantages of low storage cost, large storage capacity and offline processing with chain integrity, so as to promote the large-scale development and implementation of DApp.

13. AnnChain is a new consortium blockchain based on PBFT algorithm, which innovatively provides a more complete smart contract, hybrid consensus and encrypted computing system, and further improves the privacy protection and computing capability of the new generation of public blockchain by the original encrypted computing layer. Moreover, its smart contract has the advantages of strong enforceability, fast execution speed and built-in storage model. And data security is improved through the combination of "Oracle-Business Preprocessor-Smart Contract Processor" and hardware solutions such as SGX, which is suitable for application scenarios with high security requirements and high-frequency financial trading.

5.1.2 Application status and development trend of blockchain smart contract

The reason why blockchain can subvert the tradition lies in the three characteristics of data tamper proof and traceability, collective data maintenance and multi centralized decision-making formed by the integration of the five elements that are two structures, two algorithms and one contract, as well as the five full genes of that are full airspace, full process, full scene, full analysis and full value [82–84]. The application of blockchain can be divided into two categories based on the above characteristics: one is the extension of digital currency application, collectively referred to as Digital Assets; the other is in the real economy, government, medical, financial, agricultural, supply-chain and other fields. However, there are still pain points in the application process as an emerging technology. Nowadays, there are still three problems in the application research of blockchain smart contract as follows:

1. Ternary Paradox: the balance of scalability, distribution and security;
2. Safety Supervision: blockchain projects are not only blooming everywhere but good and bad are intermingled, which brings about the supervision is difficult;
3. Consensus Cost: the consensus mechanism of tradition frequently shows that if the cost does not go up, the efficiency will decline.

At present, there are some problems in the research of blockchain in China.

It is not easy to obtain consensus on the chain at this stage due to the greater the degree of freedom, the higher the cost of consensus [85, 86]. Nevertheless, with the strong support of the government and the unremitting efforts of the international blockchain research team, blockchain technology has developed rapidly. Industry giants have developed valuable blockchain technologies, and committed to solve the existing problems of blockchain, which injected fresh blood into the development of global blockchain.

As a kind of distributed-data technology of value Internet, blockchain has flourished from the bottom and became a new generation of information technology highly valued by governments all over the world. Blockchain technology needs to get rid of the identity of just a kind of distributed-accounting technology, and not only fully integrate with emerging information technologies such as big data, IoT and artificial intelligence, but also constantly penetrates into application scenarios of various industries, so as to promote application innovation under the integration of blockchain and new technologies [87]. In terms of innovation and application, it can attach importance to research and development from four aspects as following:

1. To promote the governance innovation of smart society;
2. To promote the development of industrial Internet and intelligent manufacturing;
3. To promote the transformation of the energy utilization and the energy industry;
4. Facilitating to build a new engine for the development of the financial industry.

Ecological construction of global blockchain ecology is still in the stages of development, but as the key development strategies of various countries, the research value of it is immeasurable. International organizations continue to promote the creation of blockchain ecology. The open-source projects of blockchain represented by Bitcoin, Ethereum and EOS have been continuously promoted, making the industrial ecology of blockchain maturation [88]. The Hyperledger Project initiated by the Linux foundation has become a key representative of the blockchain industry ecology. According to the current situation, the future development trend of blockchain-smart contract can be divided into five aspects:

1. Pragmatic governance model. Namely, develop more models and methods of governance to ensure security and controllability of blockchain markets;
2. Improve the high degree of interconnection between different chains, meanwhile, the interoperability between chains needs to realize on the premise of ensuring security;

3. Adjacent technology is closely combined with blockchain to create greater advantages. In other words, integrate emerging technologies (such as IoT) with blockchain to improve the closeness of blockchain application scenarios;
4. Use verification tools to crack down on fraudulent data sources. This needs to confirm the fraudulent data and ensure that the data got or sent on the Internet will not be obtained or tampered maliciously;
5. Continuously explore and improve the digital currency ecosystem to achieve the new development of central banks in the field of digital currency.

The innovative development and wide application of blockchain technology had become an important core of the transformation of social life and the production mode to digital. Whether blockchain can get higher development depends on three factors: cognition, technology and policy. Today, the application of blockchain technology has extended to fields [89, 90], such as epidemic-control, intelligent health care, digital finance, energy blockchain, IoT, intelligent manufacturing, supply chain management, digital asset trading and others. Certainly, the implementation of the main functions of blockchain, such as distributed shared-ledger, cryptographic algorithm, the consensus mechanism, incentive-layer, contract-layer, data-layer, network-layer, as well as traceability, provability, persistence and authoritative guarantee, is also the key technology and challenge [91, 92].

5.2 Blockchain oracle

As a closed system environment with deterministic, blockchain is separated from the real world [93]. The blockchain can only obtain the data in the chain but not out of the chain, which the main reason is that smart contract can only passively accept but cannot actively obtain the data out of the chain. In addition, it is mostly used for the transaction processing of digital assets when blockchain is applied to finance, and the required data comes from within the chain. However, non-financial applications such as supply-chain and IoT need to obtain off-chain data (that is, the data of the real world) when carrying out, and smart contracts do not support external requests. Therefore, Blockchain Oracle [94] came into being. Blockchain Oracle is the link of data exchange between blockchain and the real world, and essentially is the interface and the only way for smart contract to interact with the external world [95]. Being an off-chain component, Blockchain Oracle transmits the off-chain data as the trigger condition of smart contract to the blockchain through a specific communication channel (such as platform or sensor), which providing data services for smart contract and making it can respond to the real world that with uncertainty.

The operative mechanism of Blockchain Oracle is shown in Fig. 15. In order to ensure the determinacy of the blockchain, smart contract usually can only access the data previously stored on the blockchain, but cannot use

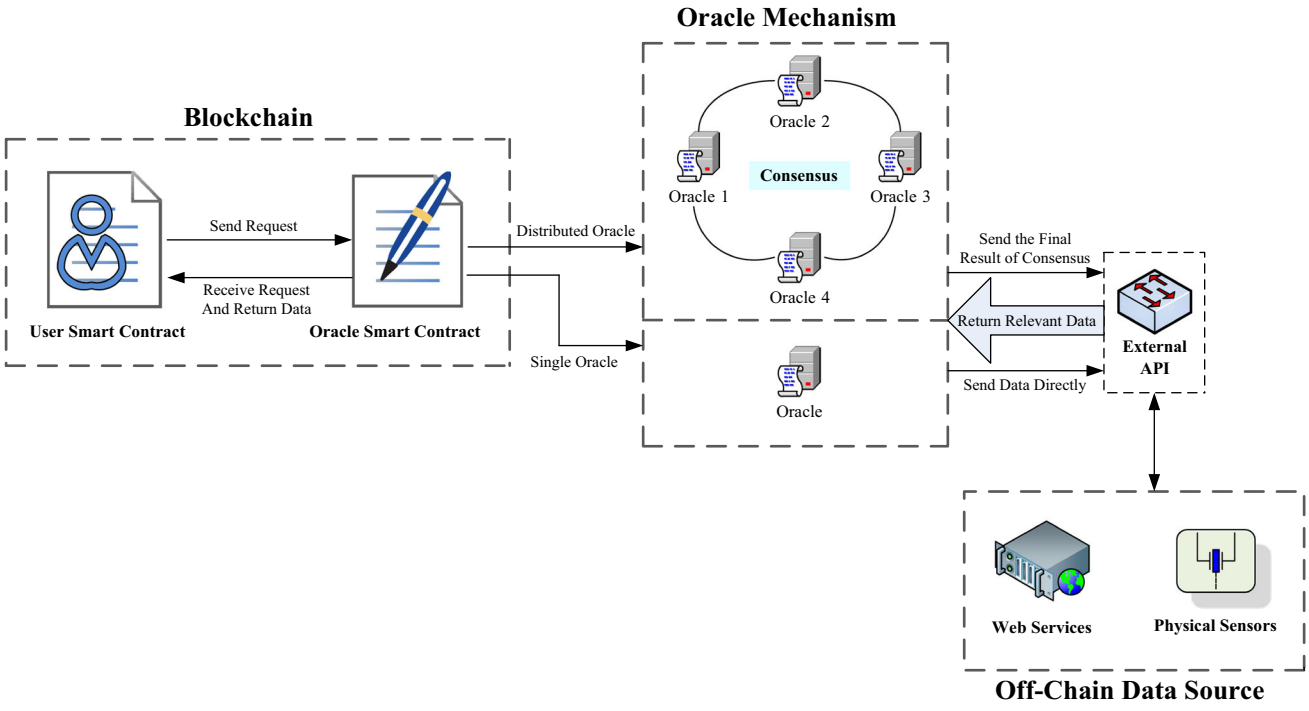


Fig. 15 Operation mechanism of Blockchain Oracle

external data. Therefore, Oracle is needed as an off-chain data transmission tool to achieve data interaction when blockchain is applied in the real world [96]. On the blockchain, the user smart contract sends the request to the Oracle smart contract, and the Oracle smart contract with the function of automation runs the corresponding Oracle mechanism according to the request in order to interact with the external API. Furthermore, the external system can directly transfer data with the blockchain if a single Oracle mechanism is running, but if running multiple distributed Oracle mechanisms, it is needed to use the consensus agreement to reach the final outcomes, and transfer the final outcomes to external API to achieve the interaction of distributed data. Once the automated Blockchain Oracle is successfully deployed, it will communicate with the off-chain data source to collect the required data, and the requester will be able to see the data when executing the user smart contract. Blockchain generally needs the assistance of Oracle in the implementation of practical applications, such as supply-chain and Internet of things, therefore, the off-chain data sources are mainly web servers and physical sensors.

Blockchain Oracle is a bridge for data interaction between blockchain and the real world, and all DApps that need off-chain data interaction require applying Oracle [97]. At present, smart contract is developing connectivity under the chain, and Blockchain Oracle as the core technology lays a solid foundation for the next generation of smart contract [98]. However, there are few research projects in the blockchain Oracle field, and the solutions of each project are different. The current mainstream Blockchain Oracle projects are shown in Table 8.

The analysis of typical Oracle projects in Table 8 is as follows:

1. ChainLink is the first decentralized Oracle solution in Ethereum, as well as the only decentralized Oracle network with high reliability that is online in the main network. Its advantages include decentralized Oracle and data source, multiple data aggregation methods (data source, node operator and Oracle network aggregation), TEE (privacy computing and offline computing), the reputation system, Reward-Punishment mechanism and the threshold signature. However, there are some shortcomings, such as high cost of chain aggregation, poor expansibility and easy centralization of reputations based system.
2. DOS Network, an extensible Layer-2 protocol, is mainly used to solve the consistency of data feedback and delivery from the chain to the smart contract, and help the smart contract to perform the tasks of large-scale throughput computing that cannot be carried out on the chain. It has two advantages: one is that not only ensures the security of the network in logic-design, but also uses the means of economic incentives to restrict the malicious nodes; another is to improve the efficiency by dividing the node group into the engine group of random number and the working group. But there is a problem that high cost of computation when the amount of computation is large due to the use of Threshold Cryptography scheme.
3. Provable is a centralized Oracle with authenticity proof, that is to prove that the data obtained from the original data source is true and not tampered with. Its advantage is that the data provider can be compatible with the blockchain protocol without modifying its service, and smart contract can directly access the data from the website or API, which has the characteristics of cost-effective, good user experience and high timeliness. Nonetheless, there are some shortcomings such as whether the verifier is credible, SPOF (single point of failure) and poor scalability.
4. Band Protocol is an Oracle platform of cross-chain data that aggregates factual data and connects it to smart

Table 8 The mainstream projects of Blockchain Oracle

Project name	Compatible platform	Oracle mechanism types	Consensus	Key technologies
ChainLink	Ethereum, Bitcoin, Hyperledger Fabric, etc	Decentralization	Threshold signatures	Reputation Contract, Order Matching Contract and Aggregation Model
DOS Network	Ethereum, EOS, TRON, ThunderCore, etc	Decentralization	Voting	Verifiable Random Function and Threshold Cryptography
Provable/ Oraclize	Ethereum, Hyperledger Fabric, EOS, R3 Corda, etc	Centralization	N/A	TLS-Notary Proof, Qualcomm TEE and Intel SGX
Band Protocol	Ethereum and Cosmos	Decentralization	Threshold Signatures	Economic Game Mechanism and Multi Currency Design
OracleChain	EOS	Decentralization	PoRD	PoRD (Poof-of-Reputation & Deposit) and OCT Token Mechanism

contracts. It is specifically defined as the middleware protocol of Layer-2, which is dedicated to provide a decentralized Oracle with faster contract-calls, cheaper service-charge, easier integration and scalability for the blockchain. And its advantage is to ensure the generation of reliable, accurate and secure data sources through the unique multi token model and equity pledge mechanism. However, Band Protocol still has a lot of room for development as Web3 is still in its early stage.

5. Oraclechain is the first decentralized Oracle solution on EOS, providing a platform for efficient access to data outside the chain in the EOS ecosystem. And its advantage is that it adopts the self-developed PoRD mechanism, which can not only realize the functions of forecasting market applications such as Augur and Gnosis, but also support the smart contract business with higher frequency access requirements for off-chain data. In addition, the service of random number proposed by OracleChain effectively solves the problems of transparency and efficiency. But the system of single reputation is prone to centralization.

Currently, the mainstream Oracle type is distributed Oracle, which mainly adopts the following four methods to solve problems that Confidence-and Security-Building [99–101]:

1. Multiple Oracle nodes: multiple nodes need to perform together the request processing of Oracle data in order to prevent the trust problem of single node Oracle, but requiring solving the problem of data inconsistency by data aggregation method. Furthermore, common aggregation algorithms include BFT consensus algorithm or the threshold signature algorithm.
2. Submission-Disclosure mechanism: Data broadcast between Oracle nodes will bring Free-loading problem, which is a Oracle does not obtain data by accessing the data source, but copies the responses of other Oracle. The Free-loading problem can be solved through the Submission-Disclosure mechanism. In addition, the Oracle node submits data answers in two stages, which the answers submitted are encrypted in the first stage, and all the answers are decrypted only after receiving enough Oracle answers.
3. Multiple data sources/trusted single data source: it is difficult to solve the integrity of data source owing to the unsafe data may give rise to Oracle to return an error result Using multiple data sources to access data can prevent the evils of a few data sources to a certain extent, but this approach is not universal because not every piece of data has multiple external data sources.
4. Benefit distribution: decentralized Oracle needs to design a set of incentive mechanism to reward and punish Oracle nodes. In the problem of Free-loading, once the node is found to have Free-loading behavior in the Submission-Disclosure stage, it is necessary to deduct its pledged deposit according to a certain proportion.

The next generation of smart contracts will contain two equally important modules with different functions, namely, on-chain and off-chain modules. The on-chain module refers to the blockchain, which has the characteristics of high reliability and decentralization, and can handle legal disputes, payment on the chain and other transactions that need to be highly transparent. The off-chain module can be implemented through Blockchain Oracle, and developers can use Oracle network to complete various off-chain tasks, which includes two-way data transmission between the on-chain contract and external system, and configuration of computing capability based on the specific requirements of both parties. Thus it can be seen that Blockchain Oracle provides many key solutions for developers and promotes the development of the next generation of smart contracts. For all that, Blockchain Oracle still needs to pay attention to the following three factors in practical application:

1. Integrity. It ensures the transmission of information to complete, accuracy and credibility, and has not been maliciously damaged or tampered with. Furthermore, integrity, it is mainly guaranteed through multiple data sources, multiple Oracle, the reputation system, trusted execution environment and the authenticity proof.
2. Confidentiality. It refers to the content of requests from smart contract to Oracle that will not be disclosed. Moreover, for confidentiality, the Oracle node uses the public key to encrypt the content of requests, as well as restricts the information flow of Oracle, and only decrypts when querying the information source.
3. Availability. It refers to the ability to get the required information in time when accessing data through Oracle, and includes achieving the function of censorship resistance. Furthermore, decentralized Oracle can effectively resolve the problem of availability.

With the continuous development of blockchain practical application, the demand for off-chain data is growing, and the importance of Oracle is becoming more and more prominent. In order to ensure availability, Blockchain Oracle not only helps developers solve the issues of interoperability, trust and scalability, but also requires solving the problems of private data security and anti-hacker attack. In addition, being an important infrastructure of blockchain, whether Blockchain Oracle can indeed and comprehensively develop depends on the demand and payment ability of the contract on the chain for the off-

chain data [101]. In the long haul, Oracle will be the integrator of all kinds of data, information, credit and assets in the real world. Moreover, the correctness of data, the decentralization of technology implementation and the intellectualization of module script that Oracle offers will have a significant impact on the connection between the future blockchain world and the real world. Therefore, Oracle Technology still needs to be continuously developed and improved.

5.3 Application status

Blockchain smart contract has broad application area, as shown in Fig. 16. According to Fig. 16, this Section will take Ethereum and Hyperledger Fabric development platforms as examples to introduce the relevant application of blockchain smart contract in the fields of financial transactions, IoT, medical application and supply-chain. In addition, we also discuss the fields current application and problems existing of EOS in the development stage, and further discuss the applications of blockchain smart contracts in Blockchain Oracle and other fields.

5.3.1 Financial transactions

In recent years, blockchain technology has been the focus of attention of central banks and financial institutions at home and abroad, and smart contract is the most important feature of blockchain applications. Therefore, smart contract can be used to solve fair trading or securities problems in the financial field.

In the Ethereum platform, aiming at the problem that the centralized TTP may leak the contract content, Zhang et al. [46] proposed a fair contract signing scheme for both parties based on Ethereum smart contract. In the process of contract signing, automatic smart contract is used instead of the original TTP agreement, which ensures the fairness of signing to a certain extent, however, the signature verification process cannot be accomplished directly through the smart contract. In order to address the problem that taxi

Fig. 16 Overview of research on blockchain-based smart contract

charging is completed by a third party bring about the disputes between drivers and passengers, Zhang et al. [102] proposed a secure-charging protocol for service of agent driving based on blockchain smart contract, which the protocol eliminates the existence of online third party through a publicly verifiable smart contract on both sides' blockchain, thus ensuring the fairness and transparency of the charging process, but this agreement only applies to the "one-to-one" situation. To overcome the problem that the charging displayed by the charging system of electric vehicles may be different from the actual charging power, as well as the potential security and privacy problems caused by the unreliable and opaque energy market, Sheikh et al. [103] implemented the consensus algorithm of energy security exchange to process transactions on smart contracts, but higher handling charges, and the scalability needs to be improved. The reason that public fog-node lacked the necessary visibility, transparency and trust is its services usually use manual payment, Debe et al. [104] use smart contracts to realize payment automation, so that fog node providers can monitor and measure their services and equipment to automatically pay bills, but the scalability is poor.

In Hyperledger Fabric smart contract, Hui et al. [105] proposed an extended framework of fabric in order to ensure the privacy and invariance of data in transactions and realize auditable function, which uses smart contract to realize auditable and privacy protection function, but the cost of its realization is throughput reducing 3–32% and delay increasing less than 10%. For the sake of ensuring automation, traceability and controllability of contracted construction project transactions, Faris et al. [106] developed a framework for blockchain integrated project delivery, which uses smart contract to achieve automatic reimbursement of expenses and implementation costs saving. However, there are some problems such as the single function of smart contract, poor practicability of framework and trust. In order to address the problems of high maintenance cost, easily tampered data and low security in the traditional centralized energy trading system, Zhou et al. [107] designed a decentralized energy trading system based on the consortium blockchain, which uses the collaborative architecture on and off the chain and smart contract to realize distributed trading, but lacks quantitative analysis, and the privacy ability of system still needs to be improved. Mustafa et al. [108] proposed a conceptual framework of electronic bidding based on blockchain smart contract, which uses the characteristics of blockchain to ensure transparency and fairness in the process of electronic bidding, however, there are some problems such as lack of the measures of privacy protection and the practicability analysis.

In the field of financial transactions, Ethereum has more obvious advantages in the public blockchain. In the public blockchain, besides being able to achieve procedural secured transactions and financial contracts, the synergy advantage enables the contracts in Ethereum to meet different functions, which each application built on Ethereum can theoretically use the functions provided by other applications. Furthermore, Hyperledger Fabric is more suitable for dealing with transactions on the consortium blockchain. Since the release of the formal version, Fabric has been favored by a lot of financial institutions, which many banks, including state-owned banks, use fabric to build the consortium blockchain and realize business innovation based on blockchain. Both platforms have their own merits, but the key is to address the problems of privacy protection and scalability.

5.3.2 Internet of Things

At present, the Internet of things (IoT) contains billions of nodes sharing data through the Internet. Through the application of the integration of Internet of things, blockchain and smart contract technology, smart contracts can be used to to create an economic application with serving the market, decentralized and shared, between devices, and take into account the privacy and the value of digital assets, thus to promote the sharing of services and resources.

Based on the Ethereum development platform, in order to solve the problems of untimely processing in the process of automobile insurance processing, Lamberti et al. [109] proposed a system to realize on-demand insurance using smart contract and sensor data. Sensors can be used to detect the degree of damage, and smart contract can be used to automatically trigger compensation, but the customer's privacy takes the risk of being disclosed. Aiming at the problem of identity management in the IoT, Omar et al. [110] proposed an identity management framework for the IoT based on semi decentralized blockchain, which uses smart contracts to implement the processes and rules of the interaction between control devices, but the delay in transaction processing will cause certain restrictions of management. Many applications in the IoT rely on the machine to machine communication, but machine to machine applications faced three challenges that is transparency, lifetime and trust, to meet this challenge, Levis et al. [111] studied the possibility and limitations of using smart contracts for the machine to machine communication by designing, implementing and evaluating AGasP, the automatic purchasing gasoline application, which proved that the use of smart contracts can improve the transparency and prolong the lifetime, and allow applications to minimize the demand for trusted third-parties, nonetheless, owing to the transaction throughput of smart contract is

lower, which limits the types of applications that can be supported. Kouzinopoulos et al. [112] introduced an application in the form of protocol to enhance the trust of users in the IoT environment of GHOST project, which uses the architecture of front end combining with rear end to ensure the data integrity in the distributed decision-making process by interacting with a group of smart contracts deployed on the private Ethereum network, so as to promote the trust of users, but the security needs to be strengthened.

Based on the Hyperledger Fabric development platform, Jawad et al. [113] proposed a blockchain based IoT architecture to address the problem of increased overhead and data delay when business continuity is applied to the IoT, which introduces an execution sequence technology for transactions to separate the execution of transactions from consistency, thus improving efficiency, but does not consider the issue of privacy and security. For constructing an efficient, safe and reliable data exchange mechanism between the independent smart toy data platform and other IoT systems, Yang et al. [114] used smart contract to solve the problem of automatic maintenance of tamper proof, reliable and distributed ledger under the premise of mutual distrust among participants, but with lower scalability. In order to provide decentralized authorization for restricted IOT devices, Vasilios et al. [115] proposed an application model based on the combination of smart contract and interleaving apparatus mechanism, but it has the problems of higher execution cost and lower throughput. To address the problems of single point of failure and data tampering in the methods of traditional access control in the IoT environment, Zhang et al. [116] designed Internet of things access control system based on smart contract, which made the system more flexible on the basis of address this problem, but the privacy of access control strategy still needs to be enhanced.

The emergence of blockchain smart contract provides a choice for IoT application development needs reliability, scalability and persistence to succeed. Therefore, the application of blockchain in the IoT has a bright future, and the application of IoT will achieve the goal of 20% development using blockchain technology. However, whether the application is implemented on Ethereum or Hyperledger Fabric platform, there will still be some scalability issues and privacy security issues in addition to the stability of the system, and even the cost of executing the smart contract will become a problem to be considered. Consequently, it is necessary to solve the basic problems of life, security and realization on the premise of achieving this goal, to ensure that the "20% development" is successful, efficient and safe.

5.3.3 Medical application

The development of medical technology highly depends on the sharing of medical data such as historical cases and clinical trials Because medical data inevitably contains a large number of personal privacy data, its access and sharing have been strictly limited. In addition, it is also difficult for patients to control the access rights of their own medical data, which leads to the difficulty in ensuring their privacy. To remove this hidden danger, medical workers need to spend a lot of time and energy to submit applications to relevant departments for the review of permission, and complete data verification before data use to ensure reliability, which will lead to inefficient work, and there are risks of medical data tampering, leakage and unsafe data transmission.

In Hyperledger Fabric, it is troublesome to collect due to the dispersity of medical data, and also difficult to synchronize and access these data in real time, to overcome this trouble, Zghaibeh et al. [117] put forward a multi-layer addressing scheme based on a private multi-layer blockchain, which to initiate various requests by using smart contract, and all users in the system can access the health-related data stored in the distributed database, but lack the ability to verify the integrity of the data. For the problem of drug supply security caused by the adulteration of counterfeit drugs into the genuine supply chain, Faisal et al. [118] used Fabric structure based on blockchain technology to process the secure drug supply chain records, thus to realize the traceability of drugs, but the privacy of patients' electronic health records has the problem of leakage.

In Ethereum, for the security issues of data transaction transmission and logging in IoT devices and other remote patient monitoring systems, Griggs et al. [119] use the smart contract based on blockchain to promote the security analysis and management of medical sensors, which to analyze medical sensors in real time and record transaction metadata, but the delay may increase the response time, thus the system cannot be used for emergency response. In order to address the security problem of information generated by individuals and devices in the medical system, Hoai et al. [120] proposed a telemedicine system based on blockchain smart contract, which uses smart contract to record data and writes the abnormal data of sensors to the blockchain immediately, meanwhile, triggers the emergency contact between doctors and hospitals for timely treatment, however, the stability of the system in large-scale environment still needs to be strengthened. Aiming at the problems such as cumbersome authorization process of the medical record, lower record sharing efficiency and difficult identity verification in the current medical system, Xu et al. [121] proposed a scheme that based on the tamper-resistant of blockchain technology and combined with

asymmetric encryption technology, which the advantages of smart contract and blockchain distributed storage can be used to ensure the privacy and security of user's medical information. In the process of dealing with medical insurance, it is often pay attention to protecting the user's privacy data but ignore the data security problems when patients interact with other roles, such as insurance companies can view the user's privacy. For this reason, Xu et al. [122] combined homomorphic encryption technology with smart contract, to ensure that any sensitive data of patients will not be disclosed to unauthorized users in the interaction process, so as to strengthen the privacy protection of user data, but the excessive number of deployed smart contracts will cause the performance to degrade, and it doesn't guarantee whether the secure interaction can be carried out in malicious mode.

In the field of medical applications, blockchain smart contract is mainly used to address the privacy security of patients' medical records and data traceability, which also has the certain application value in medical insurance and drug supply chain. However, since the tremendous and complex medical data, it must measure between improving efficiency and reducing cost in order to maximize the advantages of blockchain smart contract based on solving the problems of privacy and security.

5.3.4 Supply chain

All data in the supply chain can be seen in real time through smart contract. Furthermore, taking advantage of the decentralized, tamper proof and traceability of blockchain, promotes inventory tracking at the granularity level, ensures the security and reliability of all information in the supply chain, and reduces the risk of theft and fraud.

In Ethereum, for solving the trouble of product information traceability in cross-border business of manufacturing industry, Xu et al. [123] proposed a smart management scheme of manufacturing supply-chain based on Ethereum blockchain, which uses smart contract to realize process management and the cross-chain architecture, and ensuring the compatibility, scalability and security of the system, but the throughput is low and the system performance needs to be further strengthened. For the medical treatment of COVID-19, there are problems such as inefficient, single point failure and traceability in the existing system for the treatment of forward supply chain of COVID-19 medical equipment and the waste generated by medical equipment, to solve these problems, AHMAD et al. [124] designed and implemented the COVID-19 medical equipment supply chain based on Ethereum and IPFS (interplanetary file system) and the data traceability of waste disposal, as well as to realize automatic management by using intelligent contracts, however, the confidentiality of data and the scalability of system require being promoted. Nirav et al. [125] proposed an agricultural food supply chain system (KRanTi) based on blockchain and the 5G network, in which uses smart contract to realize automatic credit payment system that is used to control the data flow of each role in the supply chain and manage order transactions, so as to ensure the traceability of farmers' financing data and product information, but the overall cost is higher.

In Hyperledger Fabric, for the lack of detection and supervision of counterfeit drugs in the drug supply chain, and the information asymmetry between investors and drug manufacturers in drug research and development, Mueen [126] proposed a Fabric based drug traceability system (Medledger), which uses chaincode to achieve the drug registration, automatically deploy the consignment contract and update drug and contract information, but need to solve the issue of data privacy, security and scalability. In order to promote information sharing among supply chain inventory management, Tobias et al. [127] proposed a decentralized information sharing model based on Fabric, which uses chaincode to manage the transaction process and realize the management of complex multi access rights, furthermore, it can ensure the implementation of privacy policy in the process of information sharing, but it is not suitable for large-scale applications owing to the performance benchmark is low, and has poor scalability. Aiming at the matter that the information stored in the existing food supply-chain only comes from a single organization, Gao et al. [128] developed a food supply chain traceability system (FSCTS) for multi enterprise transaction based on Fabric, which uses smart contract to manage the quality information of food, multi enterprise food transaction and food data flow, but the performance of server will become the bottleneck of system throughput growth.

Blockchain smart contract is mainly used to solve the issues of data transparency, information traceability and supervision in the supply chain, which can simplify the transaction process in the fields of practical application such as IoT, products supply, manufacturing and medical drugs. The application of blockchain smart contract in the supply chain can improve the transparency and accuracy of the system, which reduces cost and improve efficiency. However, it is easy to reduce the performance of system and the effect of privacy protection as the multi-level supply chain and complex multi-management elements. Besides, it is much necessary from the real-world data sources if intend to truly realize the whole process traceability of goods. Consequently, blockchain smart contract needs to be combined with Blockchain Oracle to realize the practical application in the supply chain.

5.3.5 Application of EOS

Although yet to mature, EOS technology has been applied in different fields for its advantages of no commission and high performance. Currently, the decentralized application of EOS has been implemented in the fields such as e-commerce, education, financial technology and market, among which the representative applications are EOXCommerce, Scatter, EOSfinex and Carmel. Besides, some researchers in the EOS community also use EOS technology to solve trading problems.

Based on the eosio platform, due to the high power of the lottery center, the operators may collude with some players, resulting in unfair lottery results, and the existing work cannot guarantee that the winning numbers are real and random, and lottery participants can not verify the lottery results. In view of these problems, Li et al. [129] used smart contracts to record transactions to ensure fairness, but it has the problem of lottery buyers' privacy leakage. In view of the fact that the logistics industry generally adopts the centralized architecture, which has some security problems, such as low data privacy, low degree of decentralization, low traceability and data forgery, Ren [130] designed and proposed a smart logistics platform based on blockchain, which uses EOS as the bottom layer blockchain technology to some sensitive data in the logistics industry, such as transaction information, vehicle information is stored in the job chain, to prevent sensitive data from being tampered and forged, but there are problems of high concurrency and low intelligence. Aiming at the problem that EOSIO lacks tools for data extraction and exploration, which makes the data analysis and processing difficult, Zheng et al. [131] proposed EOSIO data acquisition framework (XBlock EOS), which uses smart contract to manage internal transactions that not only provides comprehensive EOSIO data sets, but also updates on a regular basis and quickly obtains data sets, but does not provide the function of obtaining off-chain data, as well as the characteristics of EOSIO data need to be further improved. In view of the matters of large scale, high cost and single point of failure existing in the security framework that in existence, Mohsin [132] proposed a scalable, flexible and auditable RBAC smart contract based on EOSIO platform by taking advantage of the high throughput and the strong capability of data processing of EOS blockchain, which has the strong points of lightweight and low cost, but the privacy of smart contract needs to be further enhanced. To overcome the problem that the attacker uses the internal vulnerability of EOSIO smart contract to carry out malicious attacks, resulting in serious economic losses to users, Huang et al. [133] proposed a general black-box Fuzzer framework to detect vulnerabilities in EOSIO smart contract and report it by testing Oracle, which has high accuracy and scalability, nevertheless, it is still necessary to improve the efficiency of vulnerability detection for complex smart contracts.

In addition, For the privacy security problem caused by over reliance on cloud-service providers in data sharing management platform, Gao et al. [134] proposed a blockchain based personal data security sharing scheme (BSSPD) by combining EOS, CP-ABE and IPFS, which realized data management and sharing by using smart contract, and maximized the decentralization of scheme by using EOS and IPFS, however, the overhead of computation is high in large-scale application. In order to solve the trouble that sensitive data is easily tampered with or leaked by hackers or cloud internal managers due to centralized access control mechanism in cloud, Yang et al. [135] put forward an access control framework for privacy protection based on blockchain (AuthPrivacyChain), which is based on EOS local test network and uses smart contract to achieve the settings such as transaction, encryption and access control permission, but the efficiency and performance of system needing to be strengthened. To solve the problem that the existing trading platform lacks the reporting of threat intelligence information and the incentive of trading process, Florian et al. [136] proposed a completely decentralized CTI sharing model and a trading platform based on EOS blockchain and IPFS DHT, which uses smart contract to achieve the incentive mechanism and the reporting function, but the performance does not reach the expected effect owing to the EOS technology is not mature enough, and private security needs to be increased. Carreno [137] developed an IoT expert system for smart city construction by using smart contract and neural network based on EOSIO ecosystem, which the operation rules of system are set through smart contract that the data interaction between the system and sensors is realized, but there are still some deviations in the realization of function.

As EOS technology is still in the development stage, the relevant research data is less, and the current technology has not achieved the expected effect. In addition, there are two main problems in EOS technology as follows:

1. The first problem is the efficiency of EOS. It was claimed that it could reach the throughput of one million TPS before the launch of EOS, but in fact, EOS has not achieved efficiency like that since it was launched. Besides, the DApp game experience on EOS is unideal cause users can obviously feel the phenomenon of lag. This means that EOS, on the one hand, has certain centralization, on the other hand, it does not improve ETH's experience. In this way, people's expectations of EOS have plummeted.
2. The other problem is centralization of EOS governance. The initial governance mechanism of EOS is as

follows: firstly, the EOS convention was adopted by referendum; secondly, the EOS master node is selected by the whole people with one coin and one ballot; lastly, the EOS transaction is voted by the master node, which more than 2/3 can pass. Therefore, it is very unlikely that the master node will attack the EOS node with the attacker in accounting. However, the reason that it forms a centralized governance mechanism is because the EOS master node has common interests in transaction. In other words, whether the EOS main network can be started or not, and what kind of code the EOS runs, are jointly determined by 21 main nodes. Consequently, if the main node does not implement the procedure in the case of universal approval, the referendum will be meaningless. Thus it can be seen that EOS transactions rely more on the decision of 21 master nodes, which is a weakness of DPOS consensus.

5.3.6 Blockchain Oracle

Blockchain Oracle is a rigid demand for blockchain practical applications. At present, many companies in the blockchain industry have built Blockchain Oracle with their own advantages. Aiming at the problems in traditional centralized cloud alliance such as quality monitoring, blind trust of SLA and quality of service monitoring, Mona et al. [138] proposed a decentralized cloud alliance model based on blockchain. Cloud requesters, providers and Oracle interact on and off the chain through smart contracts, in which Oracle acts as the agent of verification to monitor the quality of service, and report to the smart contract agent deployed on the blockchain, but the cost has not yet been estimated, as well as the authenticity between Oracle still needs to be enhanced. For the privacy problem caused by the scene of crowd-perception of traditional vehicle, Zhang et al. [139] proposed a vehicle crowd-perception data aggregation and privacy protection scheme (PRVB) based on Blockchain Oracle, in which the data of vehicle perception is obtained through Oracle and sent to the blockchain, furthermore, and the privacy protection of data aggregation on the chain is realized by smart contract, but the reliability of data needs to be improved.

Apart from the application research of the decentralized platform, researchers also optimize and expand Oracle itself. In view of the single point of failure caused by the centralization of a single Oracle server in the application of IoT based on blockchain, Sangyeon et al. [140] proposed a distributed Oracle (DiOr-SGX) based on Intel SGX for Ethereum, in which the smart contract can obtain the off-chain data through Oracle, and Oracle obtains data from external data sources through TLS communication and sends the external data to the blockchain through the reputation system, but it needs to reduce the number of times that malicious nodes are selected as Leader Oracle. For the sake of further develop the practical application of blockchain, Keerthi et al. [141] proposed a new decentralized Oracle protocol based on crowdsourcing the voting mechanism, and on Ethereum and Web3 clients, Oracle smart contract is used to implement management that member, contract and Reward/ Penalty mechanism, while on-chain smart contract is responsible for interacting with external data sources through Oracle protocols, but the performance of Oracle needs to be improved.

In the future, Blockchain Oracle will become the core technology of Blockchain 3.0 and promote the development of the next generation of smart contracts. And Blockchain Oracle will become indispensable when blockchain applications become mainstream. By using Blockchain Oracle, smart contract can access more comprehensive data sources, and then expand the application scope of it. In other words, the emergence of Oracle accelerates the implementation of mainstream applications based on blockchain smart contract technology.

5.3.7 Other applications of blockchain smart contract

In terms of privacy protection, in order to solve the problem of privacy protection in the alliance blockchain platform, Cai Liang et al. [142] took data isolation as the main idea and divided privacy protection into inter chain and intra chain. Smart contract is mainly used in intra chain privacy protection, exists in the form of privacy ledger, and protects data privacy through the combination of hash encryption and double signature technology. However, it is only suitable for privacy protection of small amount of data, and its performance is poor. There is a ubiquitous phenomenon of data centralized storage in the existing archives data management, as well as some problems such as poor security and tamper resistance. For these problems, Tan et al. [143] realized the identity authentication of digital archives and the determination of archives ownership through the combination of smart contract and digital signature technology, and combined smart contract with Interplanetary File System (IPFS) and other technologies to achieve the goal that the protection, verification, recovery and sharing of digital archives. However, there are some deficiencies that the larger the block height interval of public blockchain contract storage, the lower the degree of protection and data recovery of consortium blockchain. In the traditional transaction process, there is a lack of fairness during arbitration for the subjectivity of the middleman, moreover, has privacy security issues, to overcome these problems, Li et al. [144] proposed a fair scheme for big-data exchange based on smart contract and oblivious transfer protocol, among which smart contract is used to

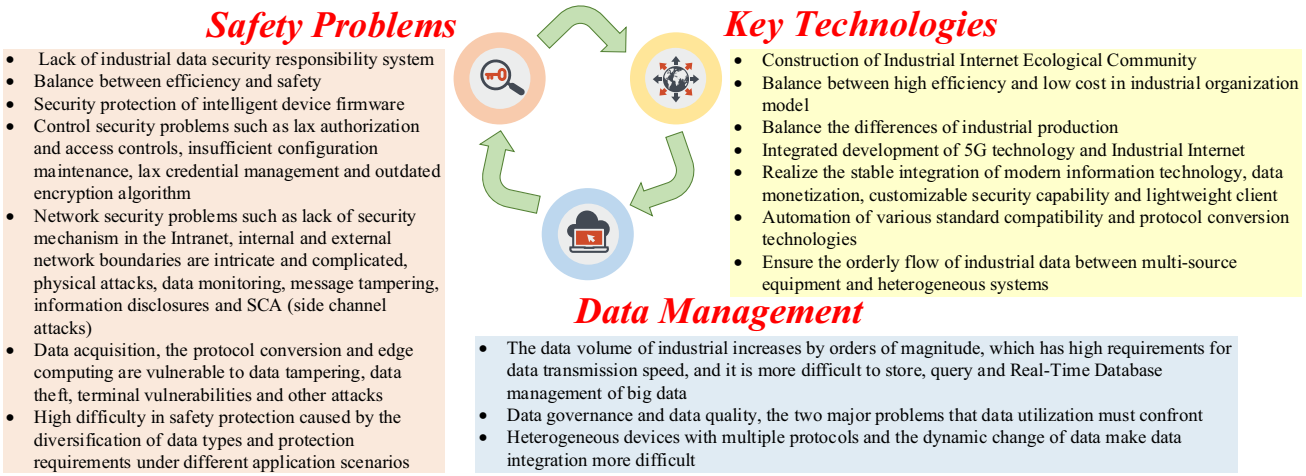


Fig. 17 Challenges faced for Industrial Internet

realize fair, autonomous and timing control of transaction, but it is a difficult problem to select appropriate n and m in m–n oblivious transmission.

Blockchain smart contract can also be used to address the problems of access control and the incentive mechanism. To effectively implement cross organization RBAC (Role-based Access Control) mechanism in the computer network, Cruz et al. [145] proposed a role-based smart contract access control mechanism (RBAC-SC), which publishes all relevant information of user role assignment in the smart contract deployed on the blockchain, and uses the Challenge-Response authentication protocol to verify whether the user has relevant roles, but privacy protection still needs to be enhanced, and has higher operation cost. Aiming at the dynamic incentive mechanism of data sharing for a large number of users in the process of data sharing, Xuan et al. [146] put forward an incentive model for data sharing based on evolutionary game theory, which deployed it on the smart contract to maintain the level of user participation by dynamically adjusting the incentive and participation cost, but ignored the influence of the size and quality of data that is shared by users.

6 Application of smart contract in industrial internet

As an important cornerstone of the fourth industrial revolution, Industrial Internet is the key to the deep integration of the new generation of information and communication technology and industrial economy, and provides a way to implement for the construction and development of the whole industrial chain and the whole value chain [147]. In recent years, driven by new theories and technologies such as mobile Internet, big data, cloud computing, artificial intelligence and blockchain, the industrial Internet has gradually shown new characteristics such as deep learning, cross-border integration, man–machine collaboration, opening crowdsensing and independent control, which is making a great impact on economic development, social progress, international politics. Moreover, it also has had a significant and far-reaching impact on the economic pattern and lifestyle [148–150]. Currently, the Industrial Internet mainly takes the centralized network architecture as the infrastructure, and there are problems such as SPOF (single point of failure), high latency, low performance and privacy security threats [151], which further hinders the transformation of industrial digitization, networking and intelligence. The advantages of Industrial Internet are steadily increasing, but it still faces the challenges shown in Fig. 17.

The emergence of cloud computing and blockchain technology provides a new solution to realize the high-level, all-round and in-depth integration of information technology and industrial system, and form a new industrial ecology with comprehensive data, intelligent application and high reliability [152–155]. Industrial Internet mainly focuses on industrial cloud, and cloud technology can meet key technical challenges and data management challenges. Nevertheless, whether it is on the cloud of equipment, the production process or operation, it puts forward high requirements for the security environment. Therefore, the key to the construction of Industrial Internet is security. Only by ensuring security can we better solve the problems of delay and efficiency. However, the introduction of blockchain technology will help to solve the security problems of applications. The ternary nature of blockchain technology (scalability, distribution and security) can solve the problems of transparency, traceability and security. The integration of blockchain technology and Industrial Internet is also a worthwhile research direction [155].

This Section will introduce the application potential of blockchain smart contract in the fields of manufacturing industry, food industry and IIoT (industrial Internet of things), and further explore the applied value of smart contract in Industry 4.0.

6.1 Manufacturing industry

After the realization of electronic and IT systems for production automation, with the emergence of CPS (cyber-physical systems) [156], the pattern of global manufacturing will also face new opportunities and challenges. Intelligent manufacturing based on the deep integration of new generation information and communication technology and advanced manufacturing technology, is a new production mode with the functions of self-perception, self-learning, self-decision-making, self-implementation and self-adaptation, which runs through all links of manufacturing activities such as design, production, management and service [157–159]. Intelligent manufacturing has become the strategic commanding point of manufacturing development, and will become the inevitable trend of manufacturing development in the future. However, although the traditional manufacturing industry is facing profound changes, it is not easy to promote intelligent manufacturing, and there are still many problems to be solved. Clarifying the direction of digital transformation, cracking the island effect, releasing data values, and promoting upstream and downstream cooperation and innovation in the industrial chain are the key problems that manufacturing enterprises need to solve for promoting digital transformation and intelligent manufacturing [157, 160, 161]. Blockchain technology, with its characteristics of development, autonomy, reliability and security, continues to promote the transformation from Information Internet to Value Internet. If intelligent manufacturing is to integrate with a wide range of social production networks and achieve the transfer of value, it is inseparable from the combination of blockchain technology [162]. The integration of blockchain technology and intelligent manufacturing brings reconstruction and innovation to the traditional manufacturing industry and realizes the digitization and networking of manufacturing.

Intelligent manufacturing mainly realizes the vertical integration of internal information systems of manufacturing enterprises, and the horizontal integration between different manufacturing enterprises based on the value chain and information flow [163]. However, multi-source heterogeneous data and centralized architecture control makes it more difficult to obtain information in real time in practical applications. In addition, all kinds of information are stored in independent systems, and there are certain differences in technical architecture, communication protocols and data storage format of each system, which will seriously affect the efficiency of interconnection and restrict the application of intelligent manufacturing in the actual production process [164]. Sensors, control modules and systems, communication networks and ERP (enterprise resource planning) systems in the manufacturing industry can be connected by using the characteristics of blockchain technology, and through the infrastructure of unified ledger, enterprises, equipment manufacturers and work safety supervision departments can monitor all links of production and manufacturing for a long time and continuously, so as to improve the safety and reliability of production and manufacturing. At the same time, the traceability and tamper proof of distributed ledger records for blockchain are also conducive to the development of enterprise audit, which is easy to find problems, track problems, solve problems, optimize the system, and greatly improve the level of intelligent management for production and manufacturing process. Applying blockchain technology to manufacturing industry mainly has the following advantages:

1. Blockchain technology can effectively collect and analyze all software and hardware equipment information existing in the independent system, further solve the problem of data island, and help the enterprise effectively establish a safer operation mechanism, more efficient workflow, and better service.
2. Data transparency and traceability with blockchain makes R & D audit, manufacturing and circulation more effective. At the same time, it also reduces operating costs, improves yield, and reduces manufacturing costs for manufacturing enterprises, so that enterprises have higher competitive edge.
3. It helps to improve the transparency and flexibility of the value chain, and can more quickly deal with the problems existing on production, logistics, warehousing, marketing, after-sales and other links.

Furthermore, the main functions of smart contract for intelligent manufacturing are shown in Fig. 18.

The integration of blockchain smart contract technology and intelligent manufacturing will effectively solve the troubles of the current manufacturing industry and further reshape the value chain. There are three main application scenarios after the integration of the two:

6.1.1 Assist in building intelligent manufacturing ecosystem

The implementation of intelligent manufacturing is a complex project promoted step by step, involving the whole life cycle of products such as design, production, logistics, sales and service, as well as the implementation

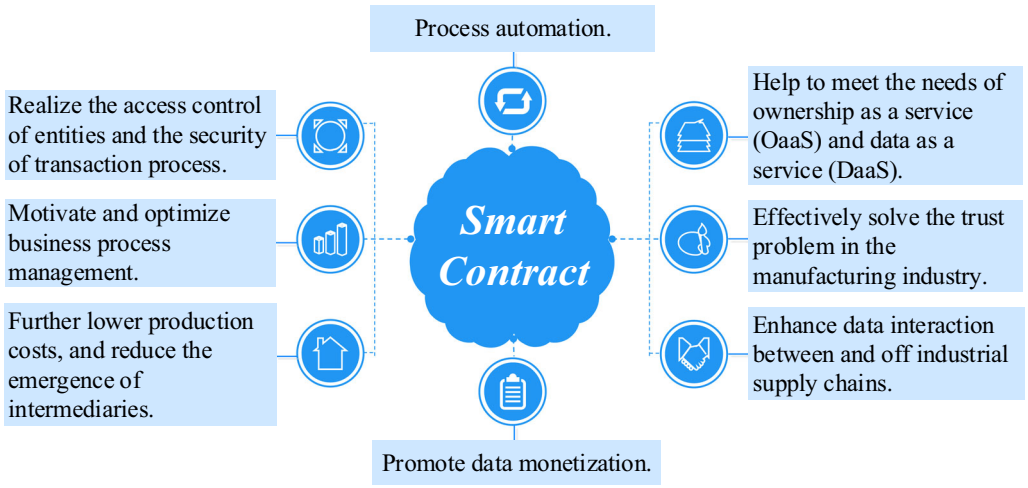


Fig. 18 Application advantages of smart contract for manufacturing industry

of enterprise system architecture such as equipment-layer, control-layer, management-layer, enterprise-layer, cloud service-layer and network-layer, which needs to realize horizontal, vertical and end-to-end integration [160, 165]. Blockchain smart contract technology can assist in the integration of artificial intelligence, 5G technology [166], edge computing [167] and other information technologies with the manufacturing industry, which is embodied in three aspects:

- Blockchain technology uses P2P networking technology and hybrid communication protocol to handle the communication between heterogeneous devices, which will significantly reduce the construction and maintenance cost of centralized data center. Furthermore, it can disperse the computing and storage requirements to each device constituting the IoT network, and effectively prevent the any SPOF in the network that resulting in the collapse of the whole network.
- The tamper proof feature of the distributed ledger with blockchain can effectively prevent the risk of information disclosure and malicious manipulation after any single node device in the IIoT is maliciously attacked and controlled.
- The combination of blockchain smart contract technology and real-time simulation technology based on digital twins is able to timely and dynamically grasp the status of various production and manufacturing equipment in the network, improve equipment utilization and the maintenance efficiency, provide accurate and efficient financial services of supply chain. Moreover, it can also help other information technologies better carry out man–machine collaboration and data processing, which jointly builds a good intelligent manufacturing system ecosystem.

6.1.2 Data security and the distributed network of intelligent production

Blockchain technology can provide enterprises with encryption services of different security levels, conduct non intermediary transmission of important data onto the manufacturing supply chain, and ensure the encryption security of important production data. With the integrated application of blockchain technology and intelligent manufacturing, the distributed network of intelligent production will be formed to promote the service-oriented transformation of the manufacturing industry dominated by the needs of end customers [168]. In addition, it can improve the efficiency of enterprise through integrated and intelligent production, and reduce the production cost of enterprises through standardized and networked production.

6.1.3 Intelligent management of manufacturing supply chain

Blockchain technology can effectively break through the data island of each link to the manufacturing supply chain, realize information sharing after data is connected to the chain, and realize intelligent decision-making based on big data analysis. Furthermore, the traceability of blockchain is conducive to tracing fake and shoddy products and recalling problematic products [169]. And smart contract technology can optimize the operational efficiency of manufacturing business, reduce transaction costs and avoid transaction risks. In addition, smart contracts can also realize the innovative application of enterprises audits, so that enterprises can not only reduce the cost of reviewing their own data and processes, but also share data with auditors. Due to the financial attribute of blockchain, it can help to manufacture enterprises to further intelligentize

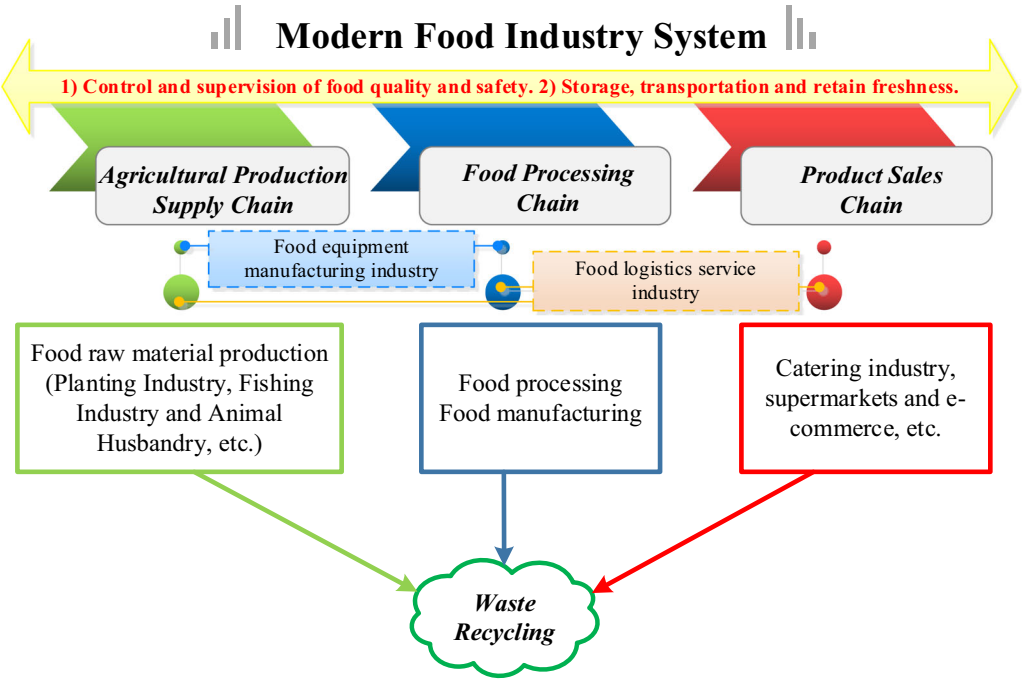


Fig. 19 Modern food industry system

their assets, realize data monetization[170] and promote the reconstruction of global value chain.

The integration of intelligent manufacturing and blockchain technology is still in its infancy, but many industrial institutions have begun to pay attention to and participate in its application exploration [171]. In the future, the new ecology of effective integration of blockchain and intelligent manufacturing will bring creative changes to the world's information technology and industrial development. The ecological platform with blockchain as the underlying technology, information oriented and demand data directly driving the manufacturing terminal will reconstruct the traditional manufacturing industry. And products will be greatly improved on a globalized and open ecological environment, so as to liberate productivity to the greatest extent and lead the global manufacturing industry to create revolutionary and brand-new production relations.

6.2 Food industry

With the rapid development of the global food industry, the food industry has gradually evolved into today's trend towards intelligence from the initial mechanization to automation. However, due to the acceleration of the vertical extension and horizontal expansion of the food industry chain, the food industry system has gradually improved, and the integrated whole industry chain operation of production, purchase, storage, processing and marketing has become a more popular business model [172]. Nevertheless, for the complex production lines in the food industry, the resulting food quality and safety cannot be ignored. The food industry Internet can be roughly divided into three parts: agricultural production supply chain, food processing chain and product sales chain, as shown in Fig. 19.

6.2.1 Agricultural production supply chain

This part is mainly composed of raw material suppliers and purchasers, involving the production process of planting, fishing and animal husbandry. In the operation process of the supply chain, suppliers mainly produce raw materials for agricultural products, record the specific production data onto raw materials and package them. After reaching a transaction consensus with the purchaser, raw materials are transported through the food logistics service industry until the purchaser confirms the receipt then completes the transaction. The intellectualization of agricultural production supply chain is mainly divided into two aspects: the intellectualization of production process and the intellectualization of raw material supply.

The intellectualization of production process refers to the use of emerging IT technology and IoT equipment to guide the prediction and implementation of production process, mainly focusing on agricultural expert system [173, 174]. There are three main indicators of the intellectualization of production process: the intellectualization of production equipment, the intellectualization of

production process optimization and management, and the intellectualization of production prediction and quality classification identification. Among them, the intellectualization of production equipment is the key to the development of the food industry and the only way to change from automation to intelligence [175]. In addition, by adding sensors to production equipment and using edge computing and other technologies, remote control and automatic operation can be realized. The automatic execution characteristics of blockchain smart contract help to improve the control efficiency, alleviate the load of agricultural producers, and reduce labor demand. Besides, specific production environment data and raw material growth status data can be obtained through the detection device, and use blockchain to save the data can assist the expert system in data analysis and decision-making, which effectively improves the production quality and production efficiency, achieve accurate operation, and reduce production cost and resource waste. Production environment is a key factor affecting the growth quality and yield of crops and livestock crops [176, 177]. Therefore, by analyzing all links in the production process and using technologies such as artificial intelligence, big data, blockchain and machine learning, it can realize accurate production decision-making, solve the problems of natural disaster, disease prevention and cost-effectiveness in the production process, and reduce production risks. The feedback information about different links can be obtained in real time through the blockchain smart contract, which can further optimize the management process of agricultural production and provide a basis of maximizing the benefits of agricultural production.

However, there are still complex risks of the intellectualization of agricultural production supply chain: poor traceability owing to uncontrollable factors such as climate; the complex production line leads to low transaction efficiency; the existence of a large number of intermediaries in supply chain transactions leads to information asymmetry and data opacity; continuous suppliers are often large-scale producers with good reputation, while weak suppliers have a single channel, which is not conducive to economic development [178]. The decentralization of blockchain technology can remove intermediaries in the agricultural value chain, reduce transaction risks and improve efficiency. Blockchain smart contract can reduce uncertainty, improve interoperability and product traceability, promote the trust building among market players, and provide more inclusive opportunities of market participation for vulnerable suppliers [179]. The main application advantages of blockchain smart contract technology in agricultural production supply chain are as follows:

1. Provide distributed database to track products, digital assets and transactions, integrate each process and transaction in the supply chain in real time, and improve the transaction efficiency.
2. Provide product traceability to ensure the authenticity of products. It can store transparent and tamper proof data, and has the potential to create efficiency gains for each participant.
3. Reduce the difficulty of monitoring and control, and reduce the frequency of fraud and misplaced transactions [178].
4. Remove intermediaries, and achieve direct interaction between suppliers and acquirers through data integration.
5. The integration of blockchain technology and intelligent devices can provide high product quality, data security and sustainable development.
6. Combine with artificial intelligence and other technologies to further improve automation and intelligence of the control system.
7. Implementing the GS1 (globe standard 1) standard in blockchain can meet the new regulations of the government and the business traceability requirements of industry regulators, and facilitate the verification of products [180].

6.2.2 Food processing chain

The food processing chain is mainly responsible for dealing with raw materials, processing and packaging them into products, and then transporting them to major sales points through the food logistics service industry. However, there are still two major problems with the food processing industry: one is the processing cost is high and consumes a lot of resources and energy, resulting in low resource utilization; but the most important problem is food safety issue. The distributed ledger, transparency, traceability and other characteristics of blockchain technology had great potential in solving food safety and resource management.

In terms of resource management, it can promote coordination and interaction among enterprises by clarifying the data format and interaction requirements of the resource information chain [181]. Analyze the best resource utilization decision through data sharing and data integration, which promotes the digitization of resource utilization and reduce the resource waste rate. In addition, due to the decentralization of blockchain, business expenses can be further saved. The multi chain architecture, cross chain technology and slicing technology of blockchain can optimize the resource allocation scheme, and automatically execute the process through smart contract to make the processing process more intelligent.

In terms of food safety, food safety incidents have occurred frequently all over the world in recent years. How to ensure food traceability and tracking has become an urgent problem to be solved. The information storage of the traditional food traceability system often uses a single database for centralized storage, which leads to the counterfeiter can tamper with the database. The existence of false data makes it difficult for the government to quickly check the source of food in case of health emergencies. The asymmetry of traceability information leads to low traceability efficiency, and the identification of false data has also become a major difficulty [182]. The opacity of food processing leads to consumers' inability to understand the source of food, which increases consumers' safety risks. The quality supervision and testing of the food industry had become the main force to control the food safety problems. The emergence of blockchain technology is expected to solve the weak points of the traditional food traceability system [183–185], and reflect the applied value of blockchain in reshaping a new information circulation and tamper proof traceability system.

Blockchain has two advantages for food safety traceability. The first is the whole process sharing of information, and the second is the easy traceability. Specific application advantages are as follows:

1. By adding raw material suppliers, processing enterprises, sales enterprises, equipment manufacturing enterprises and logistics service enterprises to blockchain, and taking advantage of the characteristics of blockchain, such as the tamper proof, data consistency and traceability, it can effectively build a consortium blockchain of government regulators, enterprise entities and third-party regulators, so as to realize the whole process sharing for all kinds of food related product information, and solve the problem of multi participant trust in the food traceability system.
2. The blockchain system can save the tamper proof records of the data processing process, and the authenticity of the data is guaranteed. Using the IoT, blockchain smart contract and encryption technology, the traceability information from food production to sales is presented to consumers. Anyone can easily trace the food information in his hand on the chain, which easily solves the problem of consumer trust.
3. Using the blockchain system to process the testing process of food testing institutions can make the testing results open and transparent, and further promote the supervision of bad behaviors in food testing.

Food safety is not only related to personal health, but also related to the stability of the whole society [186]. Although we may never be able to completely remove food-borne safety issues [187], blockchain technology will certainly bring us cost-effective transparency, and improve accountability to a new level.

6.2.3 Product sales chain

The product sales chain is mainly responsible for the business activities of processed products. In the era of the digital economy, sales business is increasingly transferred to the digital market. How to create the trust and data security of business partners and consumers, reduce operating costs and greatly improve the transaction efficiency has become the key to enterprise competition [188–190]. Blockchain has become a key factor of enterprise competition and can empower the innovation and development of enterprises. How to give full play to the great potential for blockchain in solving problems such as enterprise trusts, efficiency, cost controls, risk management and data security has become a research hotspot of digital commercial trade. The application advantages of blockchain smart contract technology in product sales chain are as follows:

1. Blockchain technology provides high security on business processes that store and transmit data. It can not only process digital asset transactions in real time, but also ensure security and accuracy.
2. The monetary characteristics can realize the digitization of assets, use smart contract to save the attributes and use standards of each asset, track the ownership and transfer of assets, and help the digital intelligence economy realize the value of token [191, 192].
3. Decentralization creates great transparency for every transaction in the sales chain, and each transaction can be quickly and conveniently added to the blockchain at marginal cost. At the same time, it reduces the transaction risk of sales.
4. The integration of blockchain and IoT can ensure the credibility, security and integrity of offline real logistics to data collection and transmission, optimize the filling efficiency and reduce the risk of cheating.
5. Improve the current situation of extensive management of commodity circulation process and shorten the cycle of commodity circulation.
6. P2P technology enables the information flow between sellers, accurately master the loss or damage of goods, and reduce the loss rate of goods.
7. The use of traceability can provide vouchers for traded goods, avoid deceptive transactions, and help to establish trust between sellers and consumers.

The digital asset trading system based on blockchain technology is still in the continuous improvement stage. In the future, blockchain can carry out research from eight aspects: basic theoretical innovation, core technology breakthrough, establishment of the standard system,

promotion of special demonstration, strengthening industry research collaboration, focusing on talent training, introduction of policy guarantee and jointly construction of good ecology, so as to help the high-quality development of digital and intelligent economy.

6.3 Industrial Internet of Things and Industry 4.0

Industrial Internet refers to networks that enable industrial interconnection, including not only the upgrading of industry, but also the upgrading of the Internet [150]. After the deep integration of industry and the Internet, a new industrial ecology using Internet thinking and information technology will be formed [193]. This ecology focuses on demand leading, innovation driven and manufacturing upgrading. Industry 4.0 refers to the fourth industrial revolution dominated by intelligent manufacturing, which aims at transforming the manufacturing industry to intelligence by making full use of the combination of information communication technology and cyberspace virtual system (such as CPS) [194]. It should be noted that Industry 4.0 emphasizes methodology, which indicates the stage of industrial development and points out that the development trend of manufacturing industry is intelligence [195]. The Industrial Internet covers the IIoT, which is the specific implementation of industry 4.0 [193]. If it wants to realize intelligent manufacturing and achieve the personalization and customization of industrial production, it must rely on the IIoT. As a new technology, under the background of Industry 4.0, how to use blockchain technology to give full play to its potential application potential and solve the key challenges in intelligent manufacturing and system security had become the key research direction of various industrial departments [196].

This Section will introduce the applied potential for blockchain in IIoT, and further analyze the guiding significance of blockchain in Industry 4.0.

6.3.1 Industrial Internet of Things

The specific definition of IIoT is that machines, computers and personnel use the advanced data analysis results obtained by business transformation to achieve intelligent industrial operation. By applying perception technology, communication technology, transmission technology, data processing technology and control technology to the industrial production process, comprehensively collect the basic data of bottom and conduct deeper data analysis and mining, so as to build a new service driven industrial ecosystem [197]. The IIoT has six characteristics: intelligent perception, ubiquitous connectivity, accurate control, digital modeling, real-time analysis and iterative optimization [198]. What's more, the use of IIoT can achieve intelligent equipment, intelligent system and intelligent decision-making. However, the operation of the IIoT still depends on the centralized architecture, which will lead to problems with security and system performance. The IIoT still faces the following challenges [151, 199–201]:

1. The disadvantages caused by centralized architecture (such as SPOF), and the huge number of equipment lead to poor robustness of the system.
2. Poor visibility of equipment and endpoints, and the difficulty of segmentation of networking environment.
3. Poor traceability of information, and inefficient data security strategy.
4. Real-time requirements, and the problem of edge training and cloud edge cooperation [202].
5. The equipment resource is constrained, and the connection between equipment is unstable and unpredictable.
6. Privacy and interoperability between heterogeneous devices, as well as deception and false authentication in data sharing.
7. The difficulty of peer-to-peer interaction caused by personalized service requirements and the standardization of complex protocols.
8. Information security in cross system interaction, and the problem of security and efficiency for the control system.
9. Ensure trust between devices and participants.

In view of the above challenges, in order to improve the Industrial Internet environment, the integration of blockchain technology into IIoT network has become a new research hotspot. Blockchain technology provides a new solution to solve the problems of standardization, traceability, auditability, interoperability, security and trust of IIoT:

1. In terms of standardization, many automation devices in IIoT use various protocols in the operation process, but these protocols do not have a set of specified standard management, that's why it is difficult to ensure interoperability between devices. The distributed ledger technology and smart contract for blockchain contributed to the implementation of standardized management. Specifically, by formulating the corresponding protocol identification for each protocol and storing it in the smart contract, it can be called during heterogeneous communication, so as to further improve the interoperability between devices.
2. In terms of traceability and auditability, all nodes in the blockchain network hold a transaction record ledger with timestamp, and users can use the corresponding timestamp to verify and track historical data records. Moreover, the tamper proof of blockchain can ensure

the authenticity of data, which it can easily detect and eliminate these bad data when the data is modified. These features provide traceability and auditability for the IIoT and promote the sharing of stored data.

3. In terms of interoperability, due to the application of interconnected heterogeneous devices in the IIoT, a lot of data will be generated, which has high requirements for interoperability. How to reduce the operation cost and complexity of deployment when improving interoperability, and further improve the bridging of shared data is a huge challenge. Blockchain technology can potentially meet this challenge. Specifically, the data types of heterogeneous devices in IIoT are stored in the blockchain after data processing such as formats conversion, processing, presentation and compression, and the corresponding data access rules and other information are stored in the blockchain. According to the same standards formulated by different entities, blockchain can also ensure the interoperability of data exchanges processes between different entities.
4. In terms of security, blockchain is based on cryptography and can use advanced encryption methods to ensure data security and privacy. And the decentralized nature of blockchain can resist security threats brought by third parties and enhance credibility. In addition, by storing the privacy protection policy and access control policy into the smart contract, which is automatically executed according to the trigger conditions, the user's data security and ownership were ensured.
5. In terms of trust, the interaction between entities in the traditional IoT depends on the centralized architecture, which cannot guarantee the trust in entities. However, blockchain technology uses distributed ledger technology and the consensus protocol to improve the transparency of data exchange. In addition, the data invariance and traceability of blockchain technology made it possible to solve the failure problems existing on the interaction between heterogeneous devices and complex information providers. The use of smart contract can achieve autonomous interaction without any third party, saving operating costs. The above functions contribute to ensuring the trust in entities in IIoT and to achieve direct interaction between entities.

In the future, IIoT technology will continue to develop with the trend of intelligent terminal, ubiquitous connection, marginalized computing, flat network and service platform, and the application potential for blockchain technology in the development trend above will continue to be tapped [200]. How to integrate and innovate blockchain technology, IIoT, 5G and other new generation digital technologies will be a major challenge, we will discuss it in Sect. 6.3.2.

6.3.2 Industry 4.0

Industry 4.0 is specifically defined as a collective term of technologies and concepts used by the organizations of value chain, and it also is a trend of using information to simplify processes and integrate automation in new technology development [203]. Its theoretical basis is the dynamic optimization of production resources within and between highly interconnected factories, and its technical basis is CPS, which aims at improving the degree of industrial autonomy and reduce the waste of human capital [204, 205]. Industry 4.0 can be roughly divided into three development stages [206–209], and the digital thinking used can be divided into three generations, as shown in Fig. 20.

The first stage of Industry 4.0 is industrial manufacturing automation. Specifically, industrial robots and industrial automation are technical power, which main purpose is to reduce human investment and finally make unmanned factories come true. At present, most factories are still in this stage. The second stage of Industry 4.0 is data flow automation. IoT, IIoT, cloud computing, big data and artificial intelligence are its technical power. Among them, IoT, as the main power, can establish digital twins [210] with the help of industrial software, such as ERP, MES, PLM and other information systems. However, only by combining cloud computing technology, big data analysis technology and artificial intelligence technology can realize real data flow automation and present the complete form of intelligent manufacturing. At present, Siemens, GE and other enterprises have basically realized digitization. The third stage of Industry 4.0 is economic operation automation, and blockchain is its driving force. Blockchain technology can effectively improve the persistence and security of IoT applications, and its smart contract can further ensure automation. In addition, blockchain technology helps to realize data monetization and further promote the development of industrial economy automation. Furthermore, in the development of Industry 4.0, it is also inseparable from the application of digital thinking. As the third generation of digital thinking, blockchain technology mainly realizes the integration of data and programs through blockchain smart contracts. If the data has its own program, it has the function of identification. The data can be used to determine the authority, and then transformed into digital assets to promote the development of digital economy. In addition, the consensus among humans, machines and different network organizations made the bottom industrial blockchain possible to support complex socio-economic operation. In the future, the digital economy with blockchain as the core will run through various application fields.

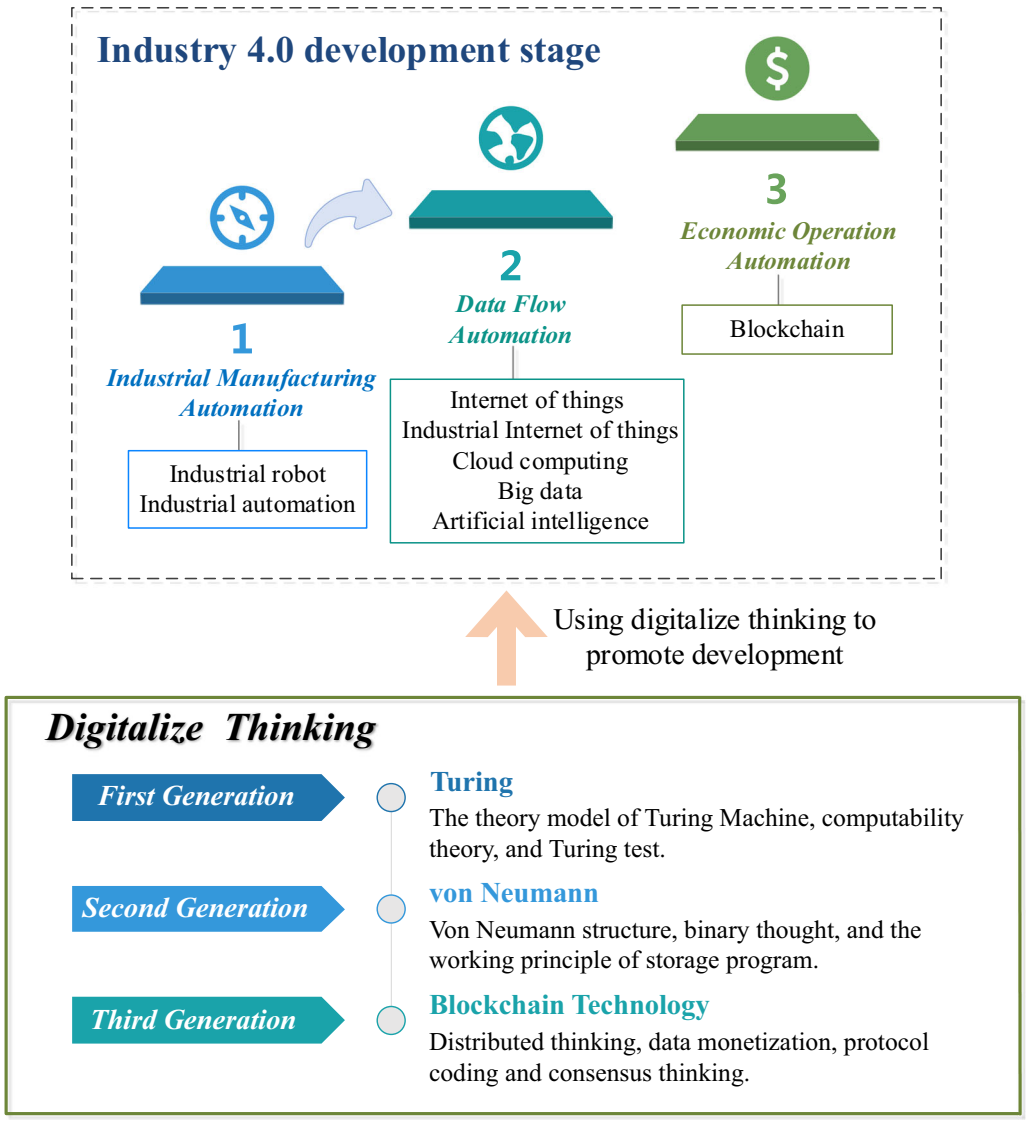


Fig. 20 Industrial 4.0 development stage and digital thinking

Application potential for blockchain smart contract technology in industry 4.0:

1. Distributed ledger and P2P technology can achieve distributed storage and shared network, and enhance redundancy and network elasticity;
2. Consensus mechanism and distributed architecture can eliminate single point of failure, realize distributed computing and provide certain fault tolerance, and ensure the security and synchronization of data. In addition, it can also promote the development of micro measurement, micro measurement, and fine-grained dynamic adjustment capabilities of intelligent manufacturing.
3. Advanced encryption and tamper proof provide data integrity, security and privacy, which improving the reliability of the system.
4. Smart contract and P2P technology can reduce the involvement of third parties, improve the trust in entities and the interoperability of heterogeneous devices, further ensure the effective connection between devices, provide the supervision mechanism and resource management function, and reduce costs.
5. Traceability, auditability and transparency promote the intelligent development of supply chain.
6. Combined with big data technology, it can improve the availability of data and provide predictability for intelligent decision-making.
7. Providing digital identity for all entities in Industry 4.0, which can promote intelligent management and realize the function of remote identification equipment;

8. Smart contract can execute heterogeneous communication protocols of the value chain of intelligent manufacturing, and automatically perform access controls, authentication and other editable logic functions. In addition, all transaction protocols can be automatically executed by smart contract, so that the transaction can be executed with the characteristics of low cost and high efficiency, ensuring the credibility and authenticity of the transaction.
9. Smart contract can provide specific storage space for applications, and smart contracts can call each other, which providing system flexibility and providing a lot of personalized manufacturing services.
10. It helps to improve the financial and trades part of industrial 4.0 ecology, provide democratic data monetization, and allow users to conduct secure micro transactions of data.
11. Combined with edge computing and the cloud platform, it can achieve distributed storage on and off the chain, and improve the robustness of system storage.
12. With the integration of artificial intelligence algorithm, cognitive configuration and operation can be realized. Using smart contract to save interaction rules can standardize cooperation and credit mechanisms between manufacturing resources. Taking blockchain as one of the additional digital twins of manufacturing process can protect the data of shared process, which promotes the development of open manufacturing ecosystem.

Blockchain smart contract technology can trigger execution when conditions are met, which reduces human intervention, making applications for IIoT more powerful and secure. Its data security will also bring additional advantages to 5G technology, big data and artificial intelligence [211–213]. However, how to integrate and innovate blockchain technology with other information technologies and give full play to its potential value of application is the biggest challenge at present. The challenges faced by the integration of blockchain technology and IIoT are as follows [214–217]:

1. Resource energy consumption: blockchain is a technology with high performance requirements, such as mining, which requires very high energy consumption. There is a great contradiction between the high energy consumption demand of blockchain and the low processing capacity of IoT equipment. In addition, the blockchain requires each node to store a sub ledger, which leads to the storage pressure caused by data expansion. Moreover, the device node itself does not have large storage capacity. Although many solutions using the cloud platform or IPFS as off-chain storage has been proposed, they cannot well solve the problem of storage pressure [154, 218, 219]. The performance of blockchain will also affect the efficiency after integration. To solve these problems, using Merkel tree for the data compression, improvement of consensus mechanism, chip technology and IOTA are the main solutions.
2. Partition tolerance problem: due to the relatively cheap IIoT equipment, there is a problem of equipment node loss caused by equipment idle or discarding. In order to ensure data consistency, it takes longer to update all node data, which results in reduced availability. At present, the main method to solve this problem is the simultaneous trading mechanism on and off the chain [220].
3. Scalability: the blockchain provides a certain degree of decentralization, security and fault tolerance at the cost of scalability. With the growth of the chain and the improvement of consensus algorithm, the demand for storage, bandwidth and computing power are also increasing. In IIoT, massive devices will generate huge amounts of data in real time, resulting in the aggravation of low throughput and scalability problems. At present, the main solutions include slicing technology, side-chain technology, storage and processing of data on off-chain, and limiting the scope of consensus for the blockchain network.
4. Security issues: the blockchain encrypts data with complex cryptography, which limits auditability and sharing governance. In addition, blockchain is still vulnerable to 51% attacks, DoS attacks and eclipse attacks [221], which hinders the progress of consensus. Therefore, the improvement of consensus mechanism is still an urgent problem to be solved. In addition, in order to prevent attackers from exploiting smart contract vulnerabilities, it is also very important to formulate security standards without security threats.
5. Communication and delay problem: blockchain technology takes P2P network as the underlying communication infrastructure, and equipment nodes need to continuously transmit and exchange data, which puts forward high requirements for the capacity and efficiency of wireless communication. In addition, due to the mobility of IIoT devices, the performance of blockchain protocol will be reduced, making it more difficult to ensure the synchronization of data between mobile nodes. The high delay of consensus mechanism hinders the development of industrial applications requiring high real-time performance.
6. Integration standard problem: at present, the integration of blockchain and IIoT is still in the primary stage, while there are many development platforms of blockchain, and the architecture and protocol existing

independently, which increases the difficulty of integration. If integration standards are not formulated, potential collaboration between different platforms will be limited, resulting in serious compatibility problems. Therefore, in order to standardize the integration process, it should focus on technical details such as non-standard heterogeneous communication protocol, equipment integration and configuration, service settings and payment, so as to build a general functional architecture of IIoT based on blockchain.

After the integration of blockchain and IIoT, the horizontal applications are mainly to open-up the whole IIoT industrial chain, improve data quality and utilization value, achieve efficient data collection and sharing, and establish a good IIoT ecology. The vertical applications are mainly in the field of intelligent manufacturing to realize the reliable, safe and efficient management of equipment identity and data. Blockchain is the digital cornerstone of the in-depth intelligent scene of IIoT. It can realize the digital integration channel of the industrial chain, strengthen the ecological consensus, promote the in-depth integration between the chain and the chain, and achieve the sustainable development of the distributed intelligent network.

7 Future research direction

7.1 Challenges for smart contract

With the popularity and application of blockchain technology, emerging smart contract technology has attracted extensive attention in academia and industry. However, on account of smart contract is limited by the performance of blockchain system itself at present, it is unable to process complex logic and high-throughput data, as well as lack privacy protection to a certain extent. Furthermore, it is still some difficulties to achieve the cross chain. Therefore, smart contracts are facing four challenges now [222]: privacy, performance, the design and security of mechanism, and formal verification, and the specific explanation for them is as follows:

1. According to the operation mechanism of smart contract, the privacy issues of smart contract can be divided into trusted data source privacy issues and contract data privacy issues, and involve the infrastructure layer and the contract layer in the infrastructure model [223]. In addition, the anonymity of blockchain does not completely solve the privacy problem of smart contract, that is because they need to ask the blockchain system to query external creditable sources when some smart contracts are executed, and these requests are usually open, and user privacy will be threatened. Consequently, it is urgent to solve the privacy security problem of smart contract, as a result of these problems of privacy may lead to anonymous attacks on blockchain or smart contract.
2. The performance problems of smart contract can be divided into two categories: the performance problems of contract caused by the design of contract layer, and the blockchain system performance problems caused by the infrastructure layer. On the one hand, the mechanism design of contract and the smart contract to be optimized will increase the execution cost and reduce the execution efficiency. On the other hand, the performance problems of blockchain system, such as low throughput, transaction delay, high energy consumption, capacity and bandwidth constraints, will also limit the performance of smart contract to a certain extent. Taking the throughput limit of blockchain system as an example, for smart contracts are executed serially in sequence in the current blockchain system, the number of contracts that can be executed per second is very limited. Moreover, smart contracts are also not compatible with the popular multi-core and cluster architecture, thus difficult to meet the needs of multi-domain applications [224].
3. The security problem in the execution-layer is the main problem that restricts the development of smart contract. This is due to smart contract deployed on the chain is irreversible, furthermore, its problems of potential security will be difficult to repair if triggered, which the resulting economic losses will be irreparable. At the same time, the anonymity of the blockchain may provide convenience for malicious users, and then result in real-world application security problems.
4. Formal verification in the operation and maintenance layer is an important method to address the security problem of smart contract, and also an important research direction of it [225]. The formal verification of smart contract refers to the use of precise mathematical means and powerful analysis tools, to verify whether the smart contract meets the expected key-properties of fairness, boundedness, correctness, realizability and non-ambiguity in the process of contract design, development and testing. Thereby to regulate the generation and execution of contracts and improve the reliability and execution, and further scale the efficient generation of smart contracts. Thus, it is an important way to address the security problem of smart contract. In addition, formal verification before contract deployment can avoid some common security vulnerabilities. There are some security checking tools for static or dynamic analysis of contracts at present, such as Oyente and Porosity. But most of these

verification tools are still in the experimental stage, and their reliability has not been verified in real systems. As a consequence, there is still an urgent need for a complete, standardized and instructive formal verification framework in the market, and it will make formal verification an important development direction of smart contracts in the future [32].

Besides the issues of smart contract itself, it also faces different challenges in the application process of different platforms, as shown below:

1. In the Ethereum platform, smart contract mainly faces the following challenges: first, it is difficult to find out where the transaction went wrong for the process of debugging a smart contract is very complicated; second, Ethereum needs manual operation to connect with other software, which will increase the burden of developers; third, Ethereum developers must build the infrastructure of Ethereum nodes individually, and it may lead to hidden risks; fourth, the update of smart contract has become an urgent problem, because the code incorporated into Ethereum that is a decentralized platform cannot be modified; Finally, building a future proof architecture is also one of the challenges must face [226].
2. In the Hyperledger platform, although the emergence of blockchain smart contract technology has a significant impact on the business model of enterprises, it also faces two challenges [227]: One is the poor scalability of the system. For the consortium blockchain system adopts efficient consensus protocol to improve the efficiency of system data processing, it leads to the limitation of system scale scalability. For instance, when the number of nodes exceeds a certain level, the system using BFT consensus protocol transmits a lot of messages between nodes, and it will result in a significant decline in the throughput of system; the other is the cost of deployment and maintenance is high. Despite the blockchain system that is geared to the needs of the consortium blockchain application design, it has a high degree of technical maturity. There are few related third-party support tools for this kind of system is not as open as the public blockchain. In addition, if they want to implement the special function of data management, consortium members require developing tools by themselves, and it will increase the cost of deployment and maintenance.
3. For EOSIO platform, EOS has a developing space in the long run. As the carrying capacity of EOS is strengthened and the development threshold is getting lower and lower, EOS has more large-scale application space. At the same time, the growth of currency price also has development space with the demand for EOS increases [228]. What's more, once the goal that the EOS virtual machine can make DApp run smoothly is realized, EOS will carry large-scale commercial applications, but the rigid demand for EOS in blockchain has not been obvious now. However, the governance of EOS ecosystem is the most difficult problem to address for the EOS program needs the master node to run. Namely, if the master node refuses to run, the program can't be executed even if it is approved by the whole people. Therefore, the complete off-chain governance cannot solve the problem of governance. Making changes in the code, such as the referendum system written into the code that the referendum to determine the branch of the program operation, may play a certain role in solving the EOS governance problem.

The tamper proof, consistency, auditability and automation of blockchain smart contract can facilitate the development of DApp. With the development of smart contract technology, the application of blockchain smart contract has been extended to IIoT, intelligent manufacturing, value chains and other fields, but its loopholes and technical problems will pose potential security threats:

1. Performance: in order to improve the performance of smart contract that limited by the performance of the blockchain system itself, the proposed Layer 2 scaling solution [229] is a feasible method to greatly improve the performance of smart contract. It creates an isolated off-chain execution environment for smart contract through cloud platforms, IPFS and other storage platforms, separating the implementation of smart contract from the consensus mechanism of the public blockchain, which achieving some on-chain operations and off-chain management, so as to conducive the realization of smart contract with high-performance, high privacy and cross chains.
2. Security: the security issues of smart contract are mainly divided into code, operating environment and the blockchain platform. There are many security problems in the contract code (integer overflow vulnerability, the restriction of gas, etc.), which is mainly solved by vulnerability detection scheme. The security problems of the operating environment mainly refer to the security vulnerabilities of the virtual machine, the docker container and image itself. The security problem of blockchain platform mainly refers to the vulnerability of encryption algorithms (reuse problem) and consensus algorithms (replay attack). To solve these problems, the security audit strategy of smart contract can be effectively solved.
3. Quantum attack: since the blockchain platform is based on cryptography, but Grover and Shor algorithms

posed an important threat to public key cryptography and hash functions [230], and affect the security of smart contract. Therefore, it is necessary to design an anti-quantum blockchain system to withstand potential quantum attacks. At present, the InterValue project has proposed a new anti-quantum attack cryptographic algorithm, but the development of anti-quantum attack blockchain is still of great significance to the security and future extended application of blockchain.

4. Standardization problem: at the legal level, the authenticity of the smart contract is insufficient (Oracle needs to provide real data), which leads to the problem that the contract is irrevocable in case of major misunderstanding. And the smart contract is not predictable, so it is impossible to predict the trend of the situation. Establishing and improving contract legal audit, combining with artificial intelligence to achieve predictability and intelligent decision-making are potential solutions. In addition, when blockchain is integrated with IIoT, it is necessary to formulate integration standards through smart contracts.
5. Intelligence: the current smart contract only realizes the function of automation and does not have intelligence. With the continuous advancement of the application of blockchain in Industry 4.0, its distributed architecture and digital assets makes it possible for the interaction between the physical world and the virtual network, and put forward the requirements of intelligent cooperation for smart contract. The integration of artificial intelligence technologies such as deep learning and cognitive computing with smart contract provides a potential possibility for the further intellectualization of smart contract.
6. Improvement of DAG-based blockchain smart contract: the unique DAG ledger structure of DAG-based blockchain not only improves the consensus efficiency, but also brings difficulties in system state migration and consistency maintenance, which brings challenges to the realization of Turing's complete smart contract. Realizing Turing complete smart contract on DAG ledger structure is facing the severe challenge that the account status may be modified by new transactions during the contract execution. At present, the main solutions are pre prevention mechanism (Vite project) and ex post rollback mechanism (InterValue project). Although the ISCP proposed by IOTA is committed to realizing functions similar to Ethereum smart contract, it is still in its infancy.

7.2 Sustainable development of blockchain smart contract

With the advent of the Industrial Internet era, Internet technology will be fully embedded in the industrial system, and will break the traditional production process, the production mode, and the management mode. As a new engine for the development of the digital economy, Industrial Internet continues to expand the new space for the development of the digital economy [231]. Artificial intelligence, 5G technology and blockchain, as the three major scientific and technological fields in the world, to promote the innovation and progress of industrial Internet. Among them, artificial intelligence is an important driving technology of Industry 4.0, and blockchain, as the main force to change data storage, has the potential to reshape the Internet and IoT. The significance of blockchain smart contract technology to the Industrial Internet is that it is expected to improve the intelligent configuration ability of production factors in all links of industrial manufacturing [210], strengthen the network collaboration between upstream and downstream of the industrial chain, and achieve man–machine collaboration based on certain rules or protocols through smart contract. Blockchain can perfectly help the Industrial Internet connect the physical world and the virtual world, and provide basic guarantee for intelligence, but its biggest bottleneck lies in how the off-chain physical world goes on-chain, which is also the technical difficulty for the further sustainable development of blockchain smart contract. In order to realize the large-scale application of blockchain smart contract technology, its future development direction is as follows:

1. Improve the execution efficiency: using WASM virtual machine to develop smart contracts can improve the security and performance of trusted execution environment, facilitate the implementation of customized services, and significantly improve the execution efficiency. However, it is difficult to learn the development language based on WASM, so use of WASM virtual machine coverage still needs to be further improved.
2. Cross chain support: combined with the cloud platform and edge technology to realize on-chain management and off-chain storage, which can improve the efficiency of automatic process execution and reduce the storage pressure of the system.
3. Optimization of encryption algorithm: encryption algorithm is not only an important factor affecting the contract performance, but also a technical difficulty. The optimization of encryption algorithm focuses on anti-quantum attack.

4. Blockchain is deeply integrated with artificial intelligence, so that the equipment nodes can interact and cooperate through smart contract, and improve the robustness and flexibility of the blockchain system.
5. Combined with ACP (artistic systems, computational experiments, parallel execution) method [232] to realize parallel organization and social management driven by smart contract.
6. Realize the deep interaction with Blockchain Oracle, but the security and credibility of the data source provided by Oracle still needs to be further improved.

However, in order to achieve the sustainable development of blockchain smart contract, it is necessary to solve the problems of social resources and energy consumption and environmental pollution caused by the mining mechanism. The basic principle of mining mechanism is PoW consensus mechanism [233]. Due to the mining machines used in mining (the ASIC mining machine of Bitcoin and the graphics card mining machine of Ethereum), it often needs to consume huge power resources. In addition, the maintenance cost of mining chips and graphics cards is also high. Obviously, energy consumption caused by mining cannot be ignored. Although the Bitcoin mining industry is transforming to clean energy, most of the power consumed by the Bitcoin network still comes from non-renewable energy, such as coal-fired power plants. As we all know, burning fossil fuels such as coal will release a large amount of carbon dioxide into the atmosphere, which is also one of the main factors of climate change. This means that the more mining computing devices join the bitcoin network, the greater the demand for the energy generation and consumption and the greater the impact on the environment [234]. At present, in order to solve the problem of energy consumption, in addition to controlling the mining scale and avoiding disorderly competition, the purpose of energy conservation and environmental protection can also be achieved by optimizing the mining mechanism.

BTC adopts mining based on PoW mechanism, which consumes a lot of computing power and power, and has 51% of the potential security risks of attack. The mining of ETH adopts PoW + PoS mechanism. Although the power consumption is low, the monetary value is not high. By improving PoS consensus, Filecoin realizes mining based on POST (proof of space time) mechanism, which is mining by putting into a lot of storage space and bandwidth resources, which is environmentally friendly and efficient. The disadvantage of PoS based mechanism lies in low security and low degree of decentralization. In addition, the prime currency proposed by Sunny King is also one of the solutions [235], which is to find the prime chain in the mining process, so that a large amount of energy consumed in the mining process can produce value cryptocurrency and improve the value of energy. For the problem of high energy consumption caused by mining, the use of renewable energy is the best solution, but it is difficult. Another solution is to realize the multi-user of energy on the basis of maintaining security.

In the future, blockchain technology will be deeply integrated with artificial intelligence, which means that productivity and production relations will change. The development of artificial intelligence, 5 g, Internet of things and other technologies will lead to security problems and public governance problems caused by the increase in the number of agents. Smart contract can deal with the transaction behavior of agents, authorize and supervise agents, and integrate fragmented individual interests effectively and at low cost. Blockchain can quantify and improve the cognitive level of nodes, provide solutions for network security, provide new impetus for overcoming collective action problems in intelligent society, and ensure the credibility and security of industrial Internet. In addition, blockchain helps to eliminate the structural holes caused by information asymmetry, establish direct links between producers and consumers, weaken the role of intermediary platform, and directly participate in economic distribution through frameworks such as deliberative democracy and agent mechanism, so as to promote the development of global value chain [236].

8 Conclusions

This paper introduces the research status of application, existing problems and solutions for blockchain smart contract. Firstly, we systematically introduce the model and operation principle of blockchain smart contract, analyzes the deployment process of smart contract based on Ethereum, Hyperledger Fabric and EOSIO, and compares the advantages and disadvantages of developing smart contract on the three platforms. In addition, we compare and analyze the blockchain with DAG-based blockchain, and introduces the deployment process of DAG-based smart contract by taking Byteball, InterValue and IOTA platforms as examples. Secondly, we summarize the application research of blockchain smart contract in the world, and further discusses the research of Blockchain Oracle, to promote the further integration of smart contract into practical application. In addition, it also analyzes the application status of blockchain smart contract based on Ethereum and Hyperledger Fabric from the fields of financial transactions, IoT, medical application and the supply chain, further discuss the application research of EOSIO platform and Blockchain Oracle. Furthermore, we introduce the application advantages and challenges of smart contract in the manufacturing industry, the food

industry, IIoT and Industry 4.0 in detail, analyze and the potential advantages of application for blockchain smart contract in industrial Internet. Finally, we expound the problems existing in the smart contract itself and the shortcomings existing in the application development process of the three platforms, analyzes the impact of large-scale application and mining system on the future development for blockchain smart contract, further introduces the social value of blockchain smart contract, and looks forward to the future research direction of blockchain smart contract.

Acknowledgements This work was supported by the Natural Science Fund of Heilongjiang Province for Outstanding Youth (YQ2019F018), the Basic Scientific Research Operating Expenses of Heilongjiang Provincial Universities and Colleges for Excellent Innovation Team (2019-KYYWF-1335), the Basic Scientific Research Operating Expenses of Heilongjiang Provincial Universities and Colleges (2019-KYYWF-1414), the Excellent Discipline Team Project of Jiamusi University (JDXKTD-2019008).

Authors' contribution LZ gave the idea, JL and LL collected data, YS and SL analyzed the data, SL wrote the paper.

Funding The Natural Science Fund of Heilongjiang Province for Outstanding Youth (YQ2019F018), the Basic Scientific Research Operating Expenses of Heilongjiang Provincial Universities and Colleges for Excellent Innovation Team (2019-KYYWF-1335), the Basic Scientific Research Operating Expenses of Heilongjiang Provincial Universities and Colleges (2019-KYYWF-1414), the Excellent Discipline Team Project of Jiamusi University (JDXKTD-2019008).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Zhang, Q. F., Jin, C. Q., Zhang, Z., Qian, W. N., & Zhou, A. Y. (2018). Blockchain: Architecture and research progress. *Chinese Journal of Computers, 041*(005), 969–988.
2. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf
3. Yuan, Y., & Wang, F. Y. (2016). Blockchain: The state of the art and future trends. *Acta Automatica Sinica, 42*(04), 481–494.
4. MIIT. (2018). The white paper on China's blockchain industry in 2018. *Chuang Ye Tian Xia, 000*(006), 7–7.
5. Worley, C. & Skjellum, A. (2018). Blockchain tradeoffs and challenges for current and emerging applications: Generalization, fragmentation, sidechains, and scalability. In *2018 IEEE international conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1582–1587.
6. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain, business & information. *Systems Engineering, 59*(3), 183–187.
7. Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K. K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications, 149*, 102471.
8. Kannengießer, N., Pfister, M., Greulich, M., Lins, S., & Sunyaev, A. (2020). Bridges between islands: Cross-chain technology for distributed ledger technology. In *Hawaii international conference on system sciences 2020*, Maui, Hawaii, January 7–10, 2020.
9. Deng, L., Chen, H., Zeng, J., & Zhang, L. J. (2018). Research on cross-chain technology based on sidechain and hash-locking. In *International conference on edge computing* (pp. 144–151).
10. Zhu, L. J. (2017). New trend in blockchain: From ethereum ecosystem to enterprise applications. In *Proceedings of the 4th global conference of knowledge economy*, Qingdao, Shandong Province, China, GCKE (pp. 1–1).
11. Shi, W. B. (2018). *The blockchain system based Hyperledger Fabric as cloud service*. Zhejiang University.
12. Luo, X. (2020). *Research and implementation of security development and debugging platform for smart contract*. University of Electronic Science and Technology of China.
13. Shen, X., Pei, Q. Q., & Liu, X. F. (2016). Survey of blockchain. *Chinese Journal of Network and Information Security, 2*(11), 11–20.
14. He, P., Yu, G., Zhang, Y. F., & Bao, Y. B. (2017). Survey on blockchain technology and its application prospects. *Computer Science, 44*(04), 1–15.
15. Yuan, Y., Ni, X. C., Zeng, S., & Wang, F. Y. (2018). Blockchain consensus algorithms: The state of the art and future trends. *Acta Automatica Sinica, 44*(11), 2011–2022.
16. Zhu, L. H., Gao, F., Shen, M., Li, Y. D., Zheng, B. K., Mao, H. L., & Wu, Z. (2017). Survey on privacy preserving techniques for blockchain technology. *Journal of Computer Research and Development, 54*(10), 2170–2186.
17. Wang, Q. G., He, P., Nie, T. Z., Shen, D. R., & Yu, G. (2018). Survey of data storage and query techniques in blockchain systems. *Computer Science, 45*(012), 12–18.
18. Ducuing, C. (2019). How to make sure my cryptokitties are here forever? The complementary roles of blockchain and the law to bring trust. *European Journal of Risk Regulation, 10*(2), 1–15.
19. Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems, 105*, 475–491.
20. Zhang, S. Y., Cheng, C., Chen, Z. M., Shi, Y. X., & Sun, D. L. (2020). Research on digital smart contract based on blockchain. *Academic Journal of Engineering and Technology Science, 3*(3), 74–80.
21. Ou, L. W., Yang, S., Yuan, Y., Ni, X. C., & Wang, F. Y. (2019). Smart contract: Architecture and research progress. *Acta Automatica Sinica, 45*(03), 445–457.
22. Northern Trust Corporation. (2019). Northern trust marks a breakthrough in securities servicing by deploying legal clauses as smart contracts on Blockchain. *Journal of Engineering*. https://www.businesswire.com/news/home/20190415005220/en/Northern-Trust-Marks-Breakthrough-Securities-Servicing-Deploying.html
23. Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law, 26*(4), 377–409.
24. Zhao, G. S., Xie, Z. J., Wang, X. M., He, J. H., Liu, X. F., Wang, X. L., Zhou, Z. H., Tian, Z. H., Tan, Q. F., & Nie, R. H. (2019). A survey on smart contract: Vulnerability analysis. *Journal of Guangzhou University (Natural Science Edition), 105*(03), 63–71.

25. Sean, W. (2018). The biggest cryptocurrency hacks in history. https://www.fool.com/investing/2018/05/09/the-biggest-cryptocurrency-hacks-in-history.aspx
26. Ren, H., & Xie, Z. Y. (2020). The criminal risk of smart contract in the era of blockchain 20 and its countermeasures—Taking the Dao hacker incident as an example. *Research on Crime and Reform, 3*, 2–7.
27. Bi, X. L., & Chen, S. (2019). The construction of "audit intelligence +" in the new era of science and technology. *Auditing Research, 212*(06), 15–23.
28. He, H. W., Yang, A., & Chen, Z. H. (2018). Survey of smart contract technology and application based on blockchain. *Journal of Computer Research and Development, 55*(11), 112–126.
29. Ba, S. S. (2017). The current situation and trend of the development of financial science and technology in China. *Tsinghua Financial Review*.
30. Li, H., Sun, J. F., Yang, Y., & Song, W. (2017). Ethereum based on blockchain 2.0. *Financial Computer of China, 000*(006), 57–60.
31. Fu, M. L., Wu, L. F., Hong, Z., & Feng, W. B. (2019). Research on vulnerability mining technique for smart contracts. *Computer Application, 039*(007), 1959–1966.
32. Cai, Y. Z. (2019). *Research and design of blockchain application development and its security verification tools*. University of Electronic Science and Technology of China.
33. Ma, C. G., An, J., Bi, W., & Yuan, Q. (2018). Smart contract in blockchain. *Netinfo Security, 215*(11), 13–22.
34. Wang, W. M., & Shi, C. Y. (2019). Intelligent contract experimental platform based on block chain technology. *Experimental Technology and Management, 036*(003), 86–91.
35. Luciano, R. B. D. S. (2018). The smart contract on gas trade: An exploratory analysis. *RAC: Revista de Administração Contemporânea, 22*(6), 903–921.
36. Shao, Q. F., Zhang, Z., Zhu, Y. C., & Zhou, A. Y. (2019). Survey of enterprise blockchains. *Journal of Software, 30*(09), 2571–2592.
37. Xia, H. F., & Xu, Q. (2020). Learning record sharing account book construction with Hyperledger Fabric technology. *Modern Electronics Technique, 43*(02), 80–83.
38. Gao, Y., & Yan, H. (2020). Middleware design in Hyperledger Fabric blockchain software architecture. *Computer & Digital Engineering, 48*(09), 2195–2200.
39. Journal News. (2018). Synacor launches BETA for Zimbra powered by EOSIO leveraging smart contracts and EOS Tokens. *Telecomworldwire*. http://www.proquest.asia/zh-CN
40. Liao, S. C. (2020). *Research on automatic security detection technology for blockchain*. University of Electronic Science and Technology of China.
41. Grigg, I. (2004). The ricardian contract. *IEEE International Workshop on Electronic Contracting, 1*(8), 25–31.
42. Huang, Y., Wang, H., Wu, L., Tyson, G., & Jiang, X. (2020). Understanding (mis)behavior on the EOSIO blockchain. In *Proceedings of the SIGMETRICS '20: ACM SIGMETRICS/international conference on measurement and modeling of computer systems*, Association for Computing Machinery, New York (pp. 83–84).
43. Yang, Q. (2018). *Research and implementation of smart contract based-on blockchain*. Southwest University of Science and Technology.
44. Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics, 35*(8), 2337–2354.
45. Lee, J. K. (2018). A docker container case study for implementing blockchain distributed general ledge. *Korean Association of Computers and Accounting, 16*(1), 27–41.
46. Zhang, L., Zhang, H., Yu, J., & Xian, H. (2020). Blockchain-based two-party fair contract signing scheme. *Information Sciences, 535*, 142–155.
47. Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks, 6*(4), 480–485.
48. Yang, X. Z., & Dong, X. W. (2019). Research and implementation of smart contract collaborative development system based on Fabric blockchain. *Journal of Nanjing University of Information Science & Technology Natural Science Edition, 011*(005), 573–580.
49. Chen, J. X. (2020). *Research and application of energy blockchain based on graphene architecture and design pattern*. University of Electronic Science and Technology of China.
50. Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). Inclusive block chain protocols. In *International conference on financial cryptography and data security* (pp. 528–547).
51. Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018). A comparative analysis of DAG-based blockchain architectures. In *2018 12th International conference on open source systems and technologies (ICOSST)* (pp. 27–34).
52. Wang, Q., Yu, J., Chen, S., & Xiang, Y., (2020). SoK: Diving into DAG-based blockchain systems.
53. Bai, C. (2018). State-of-the-art and future trends of blockchain based on dag structure. In *International workshop on structured object-oriented formal language and method* (pp. 183–196).
54. Churyumov, A. (2016). Byteball: A decentralized system for storage and transfer of value. https://byteball.org/Byteball.pdf
55. Cao, B., Li, Y. X., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z. Y., & Peng, M. G. (2019). When Internet of Things meets blockchain: Challenges in distributed consensus. *IEEE Network, 33*(6), 133–139.
56. Kim, A. & Sarin, A. (2018). Distributed ledger and Blockchain technology: Framework and use cases. *Forthcoming, Journal of Investment Management*.
57. Hilary, G. (2020). Blockchain and other distributed ledger technologies, an advanced primer. *Forthcoming, innovative technology at the interface of Finance and Operations*.
58. Chen, W., Wilson, J., Tyree, S., Weinberger, K., & Chen, Y. (2015). Compressing neural networks with the hashing trick. In *International conference on machine learning* (pp. 2285–2294).
59. Cao, Z., Long, M., Wang, J., & Yu, P. S. (2017). Hashnet: Deep learning to hash by continuation. In *Proceedings of the IEEE international conference on computer vision* (pp. 5608–5617).
60. Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The honey badger of BFT protocols. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 31–42).
61. Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance. *OSDI, 1999*(99), 173–186.
62. Yin, W., Wen, Q., Li, W., Zhang, H., & Jin, Z. (2018). An anti-quantum transaction authentication approach in blockchain. *IEEE Access, 6*, 5393–5401.
63. Li, C. Y., Chen, X. B., Chen, Y. L., Hou, Y. Y., & Li, J. (2018). A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access, 7*, 2026–2033.
64. Fernández-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access, 8*, 21091–21116.
65. Nguyen, P. Q., & Regev, O. (2019). Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology, 22*(2), 139–160.

66. Dwinger, P. (1981). Structure of completely distributive complete lattices. *Indagationes Mathematicae Proceedings, 84*(4), 361–373.
67. Gafni, A. (1988). Rollback mechanisms for optimistic distributed simulation systems. *Distributed simulation '88*.
68. Divya, M., & Biradar, N. B. (2018). IOTA-next generation block chain. *International Journal on Computer Science and Engineering, 7*(04), 23823–23826.
69. Silvano, W. F., & Marcelino, R. (2020). Iota tangle: A cryptocurrency to communicate Internet-of-Things data—ScienceDirect. *Future Generation Computer Systems, 112*, 307–319.
70. Andrieu, C., Freitas, N. D., Doucet, A., & Jordan, M. I. (2003). An introduction to MCMC for machine learning. *Machine Learning, 50*(1), 5–43.
71. Müller, S., Penzkofer, A., Kumierz, B., Camargo, D., & Buchanan, W. J. (2020). Fast probabilistic consensus with weighted votes.
72. Tanaka-Yamawaki, M., Kitamikado, S., & Fukuda, T. (1996). Consensus formation and the cellular automata. *Robotics & Autonomous Systems, 19*(1), 5–22.
73. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C. A., & Mohaisen, A. (2019). Overview of attack surfaces in blockchain. In *Blockchain for distributed systems security* (pp. 51–66).
74. Vries, L., & Vulnerability, I. O. T. A. (2019). *Large Weight Attack Performed in a Network*. University of Twente.
75. Penzkofer, A., Kusmierz, B., Capossele, A., Sanders, W., & Saa, O. (2020). Parasite chain detection in the iota protocol.
76. Bu, G., Gürcan, O., & Potop-Butucaru, M. (2019). G-IOTA: Fair and confidence aware tangle. In *IEEE INFOCOM 2019-IEEE conference on computer communications workshops (INFOCOM WKSHPS)* (pp. 644–649).
77. Ince, P., Liu, J. K., & Zhang, P. (2018). Adding confidential transactions to cryptocurrency IOTA with bulletproofs. In *International conference on network and system security* (pp. 32–45).
78. Northern Trust Corporation. (2018). Northern trust strengthens private equity audit via blockchain technology with PwC. *Journal of Engineering*. https://www.businesswire.com/news/home/20180319005240/en/Northern-Trust-Strengthens-Private-Equity-Audit-Blockchain
79. Anonymous. (2019). Ford, IBM to create blockchain for cobalt: Program will trace supply line of cobalt from Congo. *Mining Engineering*, *71*(3). http://www.proquest.asia/zh-CN
80. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLoS ONE, 11*(10), 0163477.
81. Cao, B., Lin, L., Li, Y., Liu, Y. X., Xiong, W., & Gao, F. (2020). Review of blockchain research. *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 32*(01), 1–14.
82. Ibrahim, S. A., Muhammad, I., Ian, H., & Cheung, R. C. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications, 169*(10), 179–201.
83. Boubacar, E. S., Hichem, M., Hassen, G., Abderrazak, J., & Damien, T. (2020). A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. *Sustainability, 12*(21), 9179–9198.
84. Bharat, B., Preeti, S., Martin, S. K., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers and Electrical Engineering, 90*(9), 106897.
85. Zhang, C., Wu, C., & Wang, X. (2020). Overview of Blockchain consensus mechanism. In *Big data engineering,* (pp. 7–12).
86. Han, X., Yuan, Y., & Wang, F. Y. (2019). Security problems on blockchain: The state of the art and future trends. *Acta Automatica Sinica, 45*(01), 206–225.
87. Zeng, S. Q., Huo, R., Huang, T., Liu, J., Wang, S., & Feng, W. (2020). Survey of blockchain: Principle, progress and application. *Journal on Communications, 41*(01), 134–151.
88. Saraf, C. & Sabadra, S. (2018). Blockchain platforms: A compendium. In *Proceedings of the 2018 IEEE international conference on innovative research and development (ICIRD)* (pp. 1–6), IEEE, Piscataway.
89. Ramy, O., Adrian, I., Bogdan, A., & Vasile, B. (2021). Blockchain technology—Applicability in the traceability of a product throughout the supply chain. *Macromolecular Symposia, 396*(1), 2000270.
90. Mora, H., Mendoza-Tello, J. C., Varela-Guzmán, E. G., & Szymanski, J. (2021). Blockchain technologies to address smart city and society challenges. *Computers in Human Behavior, 122*, 106854.
91. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853.
92. Li, Y., Ma, H. Y., & Wang, Z. J. (2019). Research progress on key technologies of blockchain. *Computer Engineering and Applications, 55*(20), 13–23.
93. Damjan, M. (2018). The interface between blockchain and the real world. *Ragion Pratica, 12*(01), 379–406.
94. Beniiche, A. (2020). A study of blockchain oracle, INRS. https://www.researchgate.net/publication/340662783_A_Study_of_Blockchain_Oracles
95. Caldarelli, G., Rossignoli, C., & Zardini, A. (2020). Overcoming the blockchain oracle problem in the traceability of non-fungible products. *Sustainability, 12*(6), 1–17.
96. Lo, S. K., Xu, X., Staples, M., & Yao, L. (2020). Reliability analysis for blockchain oracles. *Computers & Electrical Engineering, 83*, 106582.
97. Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information (Switzerland), 11*(11), 509.
98. Schaad, A., Reski, T., & Winzenried, O. (2019). Integration of a secure physical element as a trusted oracle in a Hyperledger blockchain. In *Proceedings of the 16th international conference on security and cryptography* (pp. 498–503), ACNS, Belgium.
99. Egberts, A. (2017). The oracle problem: An analysis of how blockchain oracles undermine the advantages of decentralized ledger systems. *SSRN Electronic Journal, 6*(18), 1–59.
100. Aldarelli, G. C. (2020). Real-world blockchain applications under the lens of the oracle problem: A systematic literature review. In *Proceeding of the 2020 IEEE international conference on technology management, operations and decisions (ICTMOD)* (pp. 1–6), IEEE, Piscataway.
101. Albreiki, H., Rehman, M., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access, PP*(99), 1–1.
102. Zhang, H., Deng, E., Zhu, H., & Cao, Z. (2019). Smart contract for secure billing in ride-hailing service via blockchain. *Peer-to-Peer Networking and Applications, 12*(1), 1346–1357.
103. Asfia, U., Kamuni, V., Sheikh, A., Wagh, S., & Patel, D. (2019). Energy trading of electric vehicles using blockchain and smart contracts. In *Proceedings of the 18th European control conference (ECC)* (pp. 3958–3963), Piscataway.
104. Debe, M., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2020). Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access, PP*(99), 1–1.
105. Kang, H., Dai, T., Jean-Louis, N., Tao, S., & Gu, X. (2019). FabZK: Supporting privacy-preserving, auditable smart

contracts in Hyperledger Fabric. In *Proceeding of the 49th annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 543–555), IEEE, Piscataway.
106. Elghaish, F., Abrishami, S., & Hosseini, M. R. (2020). Integrated project delivery with blockchain: An automated financial system. *Automation in Construction, 114*, 103182.
107. Zhou, X., Deng, L. R., Wang, B., & Pan, Z. G. (2019). Decentralized energy trading system based on consortium blockchain. *Journal of Global Energy Interconnection, 2*(06), 556–565.
108. Mustafa, M. K., & Waheed, S. (2019). A governance framework with permissioned blockchain for the transparency in e-tendering process. *International Journal of Advanced Technology and Engineering Exploration, 6*(61), 274–280.
109. Fabrizio, L., Valentina, G., Claudio, D., Matteo, P., Alfonso, G., & Victor, S. (2018). Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage. *IEEE Consumer Electronics Magazine, 7*(4), 72–81.
110. Omar, A. S., & Basir, O. (2018). Identity management in IoT networks using blockchain and smart contracts. In *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 994–1000), IEEE, Piscataway.
111. Hanada, Y., Hsiao, L., & Levis, P. (2018). Smart contracts for machine-to-machine communication: Possibilities and limitations. In *Proceedings of the 2018 IEEE international conference on Internet of Things and Intelligence System (IOTAIS)* (pp. 130–136), IEEE, Piscataway.
112. Kouzinopoulos, C. S., Giannoutakis, K. M., Votis, K., Tzovaras, D., Collen, A., Nijdam, N. A., Konstantas, D., Spathoulas, G., Pandey, P., & Katsikas, S. (2018). Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust. In *Proceedings of the 2018 innovations in intelligent systems and applications (INISTA)* (pp. 1–6), Piscataway.
113. Ali, J., Ali, T., Musa, S., & Zahrani, A. (2018). Towards secure IoT communication with smart contracts in a blockchain infrastructure. *International Journal of Advanced Computer Science and Applications (IJACSA), 9*(10), 578–585.
114. Yang, J., Lu, Z., & Wu, J. (2018). Smart-toy-edge-computing-oriented data exchange based on blockchain. *Journal of Systems Architecture, 87*, 36–48.
115. Siris, V. A., Dimopoulos, D. S., Fotiou, N., Voulgaris, S., & Polyzos, G. C. (2020). Decentralized authorization in constrained IoT environments exploiting interledger mechanisms. *Computer Communications, 152*, 243–251.
116. Zhang, J. H., Cui, B., Li, R., & Jin, J. S. (2020). Access control system of internet of things based on smart contract. *Computer Engineering*. https://doi.org/10.19678/j.issn.1000-3428.0058302
117. Zghaibeh, M., Farooq, U., Hassan, N. U., & Baig, I. (2020). SHealth: A blockchain-based health system with smart contracts capabilities. *IEEE Access, 11*(99), 1–1.
118. Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics, 8*(505), 1–32.
119. Griggs, K. N., Olya, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Thaier, H. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems, 42*(7), 1–7.
120. Pham, H. L., Tran, T. H., & Nakashima, Y. (2018). A secure remote healthcare system for hospital using blockchain smart contract. In *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)* (pp. 1–6), Piscataway.
121. Xu, J., Che, Z. D., Gong, P., & Wang, K. K. (2019). Secure storage and access scheme for medical records based on blockchain. *Journal of Computer Applications, 39*(5), 1500–1506.
122. Xu, W. Y., Wu, L., & Yan, Y. X. (2018). Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption. *Journal of Computer Research and Development, 55*(10), 2233–2243.
123. Xu, Z. J., Zhang, J., Song, Z. X., Liu, Y. C., Li, J., & Zhou, J. H. (2021). A scheme for intelligent blockchain-based manufacturing industry supply chain management. *Computing, 11*(1), 1–20. https://doi.org/10.1007/s00607-020-00880-z
124. Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., & Ellahham, S. (2021). Blockchain-based forward supply chain and waste management for COVID-19 medical equipment and supplies. *IEEE Access, 9*(9), 44905–44927.
125. Patel, N., Shukla, A., Tanwar, S., & Singh, D. (2021). KRanTi: Blockchain-based farmer's credit scheme for agriculture-food supply chain. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4286
126. Uddin, M. (2021). Blockchain Medledger: A hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics, 597*, 120235.
127. Guggenberger, T., Schweizer, A., & Urbach, N. (2020). Improving inter-organizational information sharing for vendor managed inventory: Towards a decentralized information hub using blockchain technology. *IEEE Transactions on Engineering Management, 67*(4), 1074–1085.
128. Gao, K., Liu, Y., Xu, H., & Han, T. (2020). Design and implementation of food supply chain traceability system based on Hyperledger Fabric. *International Journal of Computational Science and Engineering, 23*(2), 185.
129. Li, J., Zhang, Z., & Li, M. (2019). BanFEL: A blockchain based smart contract for fair and efficient lottery scheme. In *IEEE access* (pp. 1–8).
130. Ren, C. (2020). *Research and implementation of intelligent logistics data analysis platform based on blockchain*. University of Electronic Science and Technology of China.
131. Zheng, W., Zheng, Z., Dai, H. N., Chen, X., & Zheng, P. (2021). XBlock-EOS: Extracting and exploring blockchain data from EOSIO. *Information Processing & Management, 58*(3), 102477.
132. Rahman, M. U. (2020). Scalable role-based access control using the EOS blockchain, University of Pisa. https://www.researchgate.net/publication/342733784_Scalable_Role-based_Access_Control_Using_The_EOS_Blockchain
133. Huang, Y., Jiang, B., & Chan, W. K. (2018). EOSFuzzer: Fuzzing EOSIO smart contracts for vulnerability detection. In *Proceedings of the 2018 33rd IEEE/ACM international conference on automated software engineering (ASE)* (pp. 259–269), IEEE, Piscataway.
134. Gao, H., Ma, Z., Luo, S., Xu, Y., & Wu, Z. (2021). BSSPD: A blockchain-based security sharing scheme for personal data with fine-grained access control. *Wireless Communications and Mobile Computing, 2021*(1), 1–20.
135. Yang, C., Tan, L., Shi, N., Xu, B., & Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. *IEEE Access, 8*, 70604–70615.
136. Menges, F., Putz, B., & Pernul, G. (2020). DEALER: Decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security, 2020*(1), 1. https://doi.org/10.1007/s10207-020-00528-1
137. Carreno, R. (2021). Internet of things expert system for smart cities using the blockchain technology. *Fractals, 29*(1), 2150036.
138. Taghavi, M., Bentahar, J., Otrok, H., & Bakhtiyari, K. (2019). A blockchain-based model for cloud service quality monitoring. *IEEE Transactions on Services Computing, 13*(2), 276–288.

139. Zhang, C., Zhu, L., Xu, C., & Sharif, K. (2020). PRVB: Achieving privacy-preserving and reliable vehicular crowdsensing via blockchain oracle. *IEEE Transactions on Vehicular Technology, 70*(1), 831–843.
140. Woo, S., Song, J., & Park, S. (2020). A distributed oracle using Intel SGX for blockchain-based IoT applications. *Sensors, 20*(9), 2725.
141. Nelaturu, K., Adler, J., Merlini, M., Berryhill, R., & Veneris, A. (2020). On public crowdsource-based mechanisms for a decentralized blockchain oracle. *IEEE Transactions on Engineering Management, 67*(4), 1444–1458.
142. Cai, L., Duan, H., Yan, M., & Xia, X. (2020). Private data protection scheme for consortium blockchain based on two-layer cooperation. *Journal of Software, 31*(08), 279–295.
143. Tan, H. B., Zhou, T., Zhang, H., Zhao, Z., & Wang, W. D. (2019). Archival data protection and sharing method based on blockchain. *Journal of Software, 30*(9), 2620–2635.
144. Li, T. T., Ren, W., Xiang, Y. X., Zheng, X. H., Zhu, T. Q., Choo, K. K. R., & Gautam, S. (2021). FAPS: A fair, autonomous and privacy-preserving scheme for big data exchange based on oblivious transfer, ether cheque and smart contracts. *Information Sciences, 544*, 469–484.
145. Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using smart contract. *IEEE Access, 6*, 12240–12251.
146. Xuan, S., Zheng, L., Chung, I., Wang, W., & Guizani, M. (2020). An incentive mechanism for data sharing based on blockchain with smart contracts. *Computers & Electrical Engineering, 83*(106587), 1–12.
147. Bruner, J. (2013). Industrial internet, O'Reilly Media, Inc. http://oreilly.com/catalog/errata.csp?isbn=9781449368258
148. Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics, 14*(11), 4724–4734.
149. Lin, S. W. (2015). Industrial internet reference architecture. In *Industrial internet consortium (IIC), technical report*.
150. Li, J. Q., Yu, F. R., Deng, G., Luo, C., Ming, Z., & Yan, Q. (2017). Industrial internet: A survey on the enabling technologies, applications, and challenges. *IEEE Communications Surveys & Tutorials, 19*(3), 1504–1526.
151. Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE design automation conference (DAC)* (pp. 1–6).
152. Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry, 9*(8), 164.
153. Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., et al. (2019). Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things, 8*, 100118.
154. Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain meets cloud computing: A survey. *IEEE Communications Surveys & Tutorials, 22*(3), 2009–2030.
155. Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2021). Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wireless Networks, 27*(1), 55–90.
156. Wolf, W., & Systems, C.-P. (2009). Cyber physical systems. *Computer, 42*(3), 88–89.
157. Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: A review. *Engineering, 3*(5), 616–630.
158. Shen, W., & Norrie, D. H. (1999). Agent-based systems for intelligent manufacturing: A state-of-the-art survey. *Knowledge and Information Systems, 1*(2), 129–156.
159. Kusiak, A. (1990). *Intelligent manufacturing system*. Prentice-Hall.
160. Liang, S., Rajora, M., Liu, X., Yue, C., Zou, P., & Wang, L. (2018). Intelligent manufacturing systems: A review. *International Journal of Mechanical Engineering and Robotics Research, 7*(3), 324–330.
161. Cheng, G. J., Liu, L. T., Qiang, X. J., & Liu, Y. (2016). Industry 4.0 development and application of intelligent manufacturing. In *2016 International conference on information system and artificial intelligence (ISAI)* (pp. 407–410).
162. Viriyasitavat, W., Da Xu, L., Bi, Z., & Sapsomboon, A. (2020). Blockchain-based business process management (BPM) framework for service composition in industry 4.0. *Journal of Intelligent Manufacturing, 31*(7), 1737–1748.
163. Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology, 5*(9), 1–10.
164. Zhou, J., Li, P., Zhou, Y., Wang, B., Zang, J., & Meng, L. (2018). Toward new-generation intelligent manufacturing. *Engineering, 4*(1), 11–20.
165. Wang, B., Tao, F., Fang, X., Liu, C., Liu, Y., & Freiheit, T. (2021). Smart manufacturing and intelligent manufacturing: A comparative review. *Engineering, 7*(6), 738–757.
166. Agiwal, M., Roy, A., & Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 18*(3), 1617–1655.
167. Shi, W., Jie, C., Quan, Z., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *Internet of Things Journal, IEEE, 3*(5), 637–646.
168. Leng, J. W., Ye, S. D., & Zhou, M. (2020). Blockchain-secured smart manufacturing in industry 4.0: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51*(1), 237–252.
169. Esmaeilian, B., Sarkis, J., Lewis, K., & Behdad, S. (2020). Blockchain for the future of sustainable supply chain management in Industry 4.0. *Resources, Conservation and Recycling, 163*, 105064.
170. Opher, A., Chou, A., Onda, A., & Sounderrajan, K. (2016). *The rise of the data economy: Driving value through internet of things data monetization*, IBM Corporation, Somers, NY, USA.
171. Zhang, Q., Liao, B., & Yang, S. (2020). Application of blockchain in the field of intelligent manufacturing: Theoretical basis, realistic plights, and development suggestions. *Frontiers of Engineering Management, 7*(4), 578–591.
172. Tripoli, M., & Schmidhuber, J. (2018). *Emerging opportunities for the application of blockchain in the agri-food industry*, FAO and ICTSD, Rome and Geneva. Licence: CC BY-NC-SA, 2018, 3.
173. Xiong, H., Dalhaus, T., Wang, P., & Huang, J. (2020). Blockchain technology for agriculture: Applications and rationale. *Frontiers in Blockchain, 3*, 7.
174. Lin, J., Shen, Z., Zhang, A., & Chai, Y. (2018). Blockchain and IoT based food traceability for smart agriculture. In *Proceedings of the 3rd international conference on crowd science and engineering* (pp. 1–6).
175. Jwh, A., Min, Z. B., Wyz, A., Jhz, C., Ell, D., & Xty, A. (2021). A comprehensive review of cold chain logistics for fresh agricultural products: Current status, challenges, and future trends. *Trends in Food Science & Technology, 2021*(109), 536–551.
176. Zhao, J. C., Zhang, J. F., Feng, Y., & Guo, J. X. (2010). The study and application of the IOT technology in agriculture. In *2010 3rd International conference on computer science and information technology* (Vol. 2, pp. 462–465).

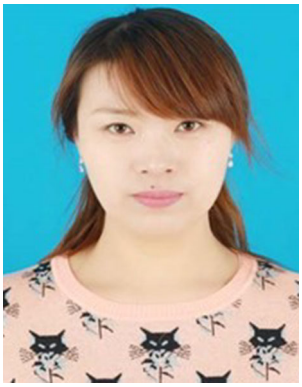
177. Benke, K., & Tomkins, B. (2017). Future food-production systems: Vertical farming and controlled-environment agriculture. *Sustainability: Science Practice and Policy, 13*(1), 13–26.
178. Kim, M., Hilton, B., Burks, Z., & Reyes, J. (2018). Integrating blockchain, smart contract-tokens, and IoT to design a food traceability solution. In *2018 IEEE 9th annual information technology, electronics and mobile communication conference (IEMCON)* (pp. 335–340).
179. Turjo, M. D., Khan, M. M., Kaur, M., & Zaguia, A. (2021). Smart supply chain management using the blockchain and smart contract. In *Scientific programming*. https://www.hindawi.com/journals/sp/2021/6092792/
180. Mba, J., Rejeb, A., Khan, N., Mba, K. D., & Hand, K. J. (2020). Optimizing global food supply chains: The case for blockchain and GSI standards—ScienceDirect. *Building the Future of Food Safety Technology*. https://doi.org/10.1016/B978-0-12-818956-6.00017-8
181. Longo, F., Nicoletti, L., & Padovano, A. (2020). Estimating the impact of blockchain adoption in the food processing industry and supply chain. *International Journal of Food Engineering, 16*, 5–6.
182. Feng, H., Wang, X., Duan, Y., Zhang, J., & Zhang, X. (2020). Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *Journal of Cleaner Production, 260*, 121031.
183. Xu, Y., Li, X., Zeng, X., Cao, J., & Jiang, W. (2020). Application of blockchain technology in food safety control: Current trends and future prospects. *Critical Reviews in Food Science and Nutrition*. https://doi.org/10.1080/10408398.2020.1858752
184. Tse, D., Zhang, B., Yang, Y., Cheng, C., & Mu, H. (2017). Blockchain application in food supply information security. *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2017*, 1357–1361.
185. Galvez, J. F., Mejuto, J. C., & Simal-Gandara, J. (2018). Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in Analytical Chemistry, 107*, 222–232.
186. Henson, S., & Caswell, J. (1999). Food safety regulation: An overview of contemporary issues. *Food Policy, 24*(6), 589–603.
187. Borchers, A., Teuber, S. S., Keen, C. L., & Gershwin, M. E. (2010). Food safety. *Clinical Reviews in Allergy & Immunology, 39*(2), 95–141.
188. Oswald, G., & Kleinemeier, M. (2017). *Shaping the digital enterprise*. Springer. https://doi.org/10.1007/978-3-319-40967-2_8
189. Olifirov, A. V., Makoveichuk, K. A., Zhytnyy, P. Y., Filimonenkova, T. N., & Petrenko, S. A. (2018). Models of processes for governance of enterprise IT and personnel training for digital economy. In *XVII Russian scientific and practical conference on planning and teaching engineering staff for the industrial and economic complex of the region (PTES)* (pp. 216–219).
190. Brusakova, I. A. & Shepelev, R. E. (2016). Innovations in the technique and economy for the digital enterprise. In *2016 IEEE V forum strategic partnership of universities and enterprises of hi-tech branches (science. education. innovations)* (pp. 27–29).
191. Fiske, K. E., Isenhower, R. W., Bamond, M. J., & Lauderdale-Littin, S. (2020). An analysis of the value of token reinforcement using a multiple-schedule assessment. *Journal of Applied Behavior Analysis, 53*(1), 563–571.
192. Malherbe, L., Montalban, M., Bédu, N., & Granier, C. (2019). Cryptocurrencies and blockchain: Opportunities and limits of a new monetary regime. *International Journal of Political Economy, 48*(2), 127–152.
193. Magomadov, V. (2020). The industrial internet of things as one of the main drivers of industry 4.0. In *IOP conference series: Materials science and engineering* (Vol. 862, No. 3, p. 032101).
194. Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering, 6*(4), 239–242.
195. Lee, J., Azamfar, M., & Singh, J. (2019). A blockchain enabled cyber-physical system architecture for Industry 4.0 manufacturing systems. *Manufacturing Letters, 20*, 34–39.
196. Mohamed, N. & Al-Jaroodi, J. (2019). Applying blockchain in industry 4.0 applications. In *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)* (pp. 0852–0858).
197. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2), 676–1717.
198. Serpanos, D. & Wolf, M. (2018). Industrial internet of things. In *Internet-of-Things (IoT) systems* (pp. 37–54), Springer.
199. Younan, M., Houssein, E. H., Elhoseny, M., & Ali, A. A. (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement, 151*, 107198.
200. Khan, W. Z., Rehman, M., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering, 81*, 106522.
201. Aazam, M., Zeadally, S., & Harras, K. A. (2018). Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Transactions on Industrial Informatics, 14*(10), 4674–4682.
202. Wang, G. *SoK: Applying blockchain technology in industrial internet of things*.
203. Davis, R., Sessions, B.-O., & Check, A. R. (2015). Industry 4.0. In *Digitalisation for productivity and growth, European Parliament, members' research service*.
204. Zhou, K., Liu, T., & Zhou, L. (2015). Industry 4.0: Towards future industrial opportunities and challenges. In *2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)* (pp. 2147–2152).
205. Lu, Y. (2017). Cyber physical system (CPS)-based industry 4.0: A survey. *Journal of Industrial Integration and Management, 2*(03), 1750014.
206. Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Industrial Electronics Magazine, 11*(1), 17–27.
207. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access, 7*, 45201–45218.
208. Bahrin, M. A. K., Othman, M. F., Azli, N. H. N., & Talib, M. F. (2016). Industry 4.0: A review on industrial automation and robotic. *Jurnal Teknologi, 78*, 6–13.
209. Alladi, T., Chamola, V., Parizi, R. M., & Choo, K.-K.R. (2019). Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access, 7*, 176935–176951.
210. El Saddik, A. (2018). Digital twins: The convergence of multimedia technologies. *IEEE Multimedia, 25*(2), 87–92.
211. Kar Af Iloski, E. & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017—17th international conference on smart technologies*.
212. Hussain, A. A., & AlUrjman, F. (2021). Artificial intelligence and blockchain: A review. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4268
213. Haris, R. M. & Al-Maadeed, S. (2020). Integrating blockchain technology in 5g enabled iot: A review. In *2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT)* (pp. 367–371).

214. Xiong, Z., Zhang, Y., Dusit, N., Wang, P., & Zhu, H. (2017). When mobile blockchain meets edge computing. *IEEE Communications Magazine, 56*(8), 33–39.
215. Iqbal, A., Amir, M., Kumar, V., Alam, A., & Umair, M. (2020). Integration of next generation IIoT with Blockchain for the development of smart industries. *Emerging Science Journal, 4*, 1–17.
216. Dinh, T. N., & Thai, M. T. (2018). AI and blockchain: A disruptive integration. *Computer, 51*(9), 48–53.
217. Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications, 149*, 102481.
218. Kumar, R., Marchang, N., & Tripathi, R. (2020) Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In *International conference on communication systems & networks (COMSNETS)* (pp. 1–5).
219. Krejci, S., Sigwart, M., & Schulte, S. (2020). Blockchain-and IPFS-based data distribution for the Internet of Things. In *European conference on service-oriented and cloud computing* (pp. 177–191).
220. Kampik, T., & Najjar, A. (2020). Simulating, off-chain and on-chain: Agent-based simulations in cross-organizational business processes. *Information, 11*(1), 34.
221. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In *24th {USENIX} Security Symposium ({USENIX} security 15)* (pp. 129–144).
222. Zhu, Y., Wang, J., Guo, Q., & Liu, G. W. (2020). Research progress of smart contracts based on blockchain. *Cyberspace Security, 11*(09), 19–24.
223. Vivar, A. L., Castedo, A. T., Orozco, A. L. S., & Villalba, G. (2020). Smart contracts: A review of security threats alongside an analysis of existing solutions. *Entropy, 22*(2), 203–232.
224. Sekhar, S. R. M., Siddesh, G. M., Kalra, S., & Anand, S. (2019). A study of use cases for smart contracts using blockchain technology. *International Journal of Information Systems and Social Change, 10*(2), 15–34.
225. Hu, K., Bai, X. M., Gao, L. C., & Dong, A. Q. (2016). Formal verification method of smart contract. *Research on Information Security, 2*(012), 1080–1089.
226. Oliva, G. A., Hassan, A. E., & Jiang, Z. M. J. (2020). An exploratory study of smart contracts in the ethereum blockchain platform. *Empirical Software Engineering, 25*(2), 1864–1904.
227. Yu, G., Nie, T. Z., Li, X. H., Shen, D. R., & Bao, Y. B. (2021). The challenge and prospect of distributed data management techniques in blockchain systems. *Chinese Journal of Computers, 44*(01), 28–54.
228. He, N. Y., Zhang, R. Y., Wu, L., Wang, H. Y., Luo, X. P., Guo, Y., Yu, T., & Jiang, X. X. (2020). Security analysis of EOSIO smart contracts. *Computer Science*. https://www.researchgate.net/publication/339971781_Security_Analysis_of_EOSIO_Smart_Contracts
229. Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). *Layer 2 blockchain scaling: A survey*.
230. Rodenburg, B., & Pappas, S. P. (2017). Blockchain and quantum computing. *The Mitre Corporation*. https://doi.org/10.13140/RG.2.2.29449.13923
231. Radanliev, P., De Roure, D., Nicolescu, R., et al. (2019). *New developments in cyber physical systems, the internet of things and the digital economy—Discussion on future developments in the industrial internet of things and industry 4.0*. https://doi.org/10.1007/s00146-020-01049-0
232. Lun, S. X. (2012). Research on the classification of parallel execution modes of ACP theory. *Acta Automatica Sinica, 38*(10), 1602.
233. Yun, J., Goh, Y., & Chung, J.-M. (2019). Analysis of mining performance based on mathmatical approach of PoW. In *2019 International conference on electronics, information, and communication (ICEIC)* (pp. 1–2).
234. Goodkind, A. L., Jones, B. A., & Berrens, R. P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Research & Social Science, 59*, 101281.
235. King, S. (2013). Primecoin: Cryptocurrency with prime number proof-of-work. *July 7th, 1*, 6.
236. Gereffi, G., & Fernandez-Stark, K. (2018). Global value chain analysis: A primer. In *Global value chains and development: Redefining the contours of 21st century capitalism* (p. 305).

Shi-Yi Lin born in 1999, received the B.E. in College of Electronic Information Engineering at Jiaying University, Meizhou, China, in 2020. She is currently a postgraduate Student in College of Information Science and Electronic Technology at Jiamusi University. Her main research interests include security and privacy in blockchain networks, smart contract, and cryptographic protocol.

Lei Zhang born in 1982, received the B.E., M.E. in College of Information Science and Electronic Technology at Jiamusi University, Jiamusi, China, in 2005 and 2011, respectively. He received the PH.D in 2018 in College of Computer Science and Technology at Harbin Engineering University. He is also a professor and the director of computer software teaching and research office in College of Information Science and Electronic Technology at Jiamusi University. His research interests are security and privacy in vehicle networks, and mobile privacy protocol. (Corresponding Author)

Jing Li born in 1968, she is a professor in College of Information and Electronic Technology at Jiamusi University, Jiamusi, China. Her research interests are machine learning and data privacy.



Li-li Ji born in 1979, received her master's degree in software engineering from Beijing University of Posts and Telecommunications in 2018. She is a lecturer of School of Economics and Management in Jiamusi University. She is also the director of Work Department of Federation of Social Sciences Science in Science and Technology Department. Her research interests include urban planning and community management. (Corresponding Author)

Yue Sun born in 1995, received the B.E., M.E. in College of Information Science and Electronic Technology at Jiamusi University, Jiamusi, China, in 2017 and 2020, respectively. She is also a teacher and the lecturer of department of robotics engineering teaching and research office in College of Information Science and Electronic Technology at Jiamusi University. She is a member of the CCF. Her research interests are security and privacy in mobile social networks.