International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain-Architecture, Applications, and Future Scope

J. C. Pasalkar[1], Aniket A. Kadale[2]

[1]Assistant Professor, Department of Information Technology, AISSMS's Institute of Information Technology, Pune-411001, INDIA
[2]TE. (Information Technology), AISSMS's Institute of Information Technology, Pune-411001, INDIA

A B S T R A C T

In recent times, the rapid-fire- fire development of cryptocurrencies and their underpinning blockchain technology has revived Szabo's original idea of smart contracts, i.e., computer protocols that are designed to automatically grease, corroborate, and apply the concession and performance of digital contracts without central authorities. Smart contracts can find a wide spectrum of implicit operation scripts in the digital economy and intelligent industriousness, including financial services, operation, healthcare, and Internet of goods, among others, and also have been integrated into the mainstream blockchain- predicated development platforms, analogous as Ethereum and Hyperledger. still, smart contracts are still far from mature, and major technical challenges analogous as security and insulation issues are still awaiting further disquisition sweats. For case, the most notorious case might be " The DAO Attack " in June 2016, which led to further than$ 50 million Ether transferred into an adversary's account. In this paper, we strive to present a regular and comprehensive overview of blockchain- enabled smart contracts, aiming at stimulating further disquisition toward this arising disquisition area. We first introduced the operating medium and mainstream platforms of blockchain- enabled smart contracts, and proposed a disquisition frame for smart contracts predicated on a new six- caste architecture. Second, both the technical and legal challenges, as well as the recent disquisition progresses, are listed. Third, we presented several typical operation scripts. Toward the end, we mooted the future development trends of smart contracts. This paper is aimed at furnishing helpful guidance and reference for future disquisition sweats. calligraphies entered on 8 November 2018. Revised December 24, 2018. Accepted on January 18, 2019. smart industriousness.

Introduction to Blockchain-Architecture, Applications and Future Scope

THE TERM "smart contract " was first chased in medial- 1990s by computer scientist and cryptographer Szabo, who defined a smart contract as " a set of pledges, specified in digital form, including protocols within which the parties perform on these pledges(1). Smart contracts go beyond the dealing machine by proposing to bed contracts in all feathers of parcels by digital means(2). Szabo also anticipated that through clear sense, verification and enforcement of cryptographic protocols, smart contracts could be far more functional than their insensible paper- grounded ancestors. still, the idea of smart contracts didn't see the light till the emergence of blockchain technology, in which the public and tack - only distributed tally technology(DLT) and the agreement medium make it possible to apply smart contract in its true sense.

Generally speaking, smart contracts can be defined as the computer protocols that digitally grease, corroborate, and apply the contracts made between two or further parties on blockchain. As smart contracts are generally stationed on and secured by blockchain, they've some unique characteristics. First, the program law of a smart contract will be recorded and vindicated on blockchain, therefore making the contract tamper- resistant. Second, the prosecution of a smart contract is executed among anonymous, unsure individual bumps without centralized control, and collaboration of third- party authorities. Third, a smart contract, like an intelligent agent, might have its own cryptocurrencies or other digital means, and transfer them when predefined conditions are touched off(3).

Motivation

1.The need for decentralization is the key motivation behind the blockchain technology.

2.Decentralization is achieved by distributing the computation tasks to all the nodes of the blockchain network.

Aim and Objective of the work

The aim of the project is to provide peer-to-peer network platform that can provide security and fasten the transaction process.

The project's objective is to achieve Decentralization by distributing the computation tasks to all the nodes of the blockchain network.

The project also focuses on bringing transparency in the transactions

We want to solve several problems of traditional systems by Decentralization.

2. A brief Intro to Blockchain

The conception of a blockchain began from Bitcoin, which is a cryptocurrency constructed by an unknown person or group of people using the alias Nakamoto in 2008(4). Blockchain adopts the P2P protocol that can tolerate a single point of failure. The agreement medium ensures a common, unequivocal ordering of deals and blocks, and guarantees the integrity and thickness of the blockchain across geographically distributed bumps. By design, blockchain has similar characteristics as decentralization, integrity, and felicity(5). According to Xu etal.(6), blockchain can serve as a new kind of software connector, which should be considered as a possible decentralized volition to the being centralized participated data storehouse.

In addition, grounded on different situations of access authorization, blockchains can be divided into three types 1) public blockchain(similar as Bitcoin and Ethereum); 2) institute blockchain(similar as Hyperledger and Ripple); and 3) private blockchain.

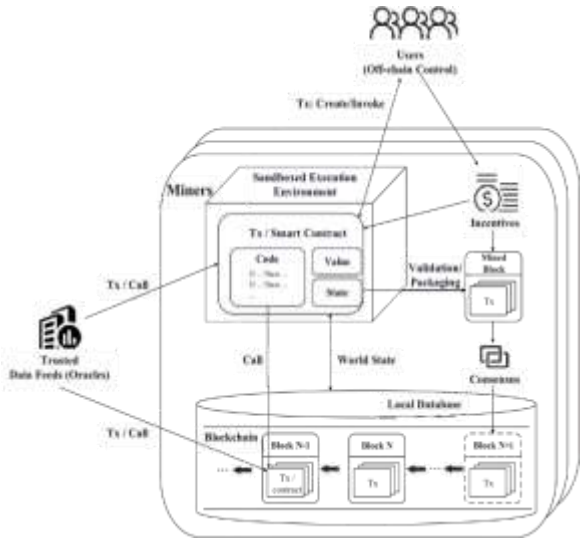

Fig. 1. Operational mechanism of smart contract.

2.1 Challenges and recent progresses

As an arising technology in its immaturity, smart contracts presently face numerous problems and challenges. Grounded on the proposed exploration frame which employs a six- subcaste armature, this section will outline the challenges and recent exploration progresses of smart contracts. Contract Vulnerabilities Contract vulnerabilities substantially appear in the contracts subcaste in the exploration frame we proposed. The vicious miners or druggies can exploit them to gain profit. Then are some typical cases(18) –(20).

1) sale- Ordering Dependence(TOD) Each block contains several deals, and the order in which deals are executed depends on the miner. TOD occurs when several dependent deals bring the same contract that the miner can manipulate the order in which the deals are executed.

2) Timestamp Dependence The miners set the timestamp for the block they booby-trapped(generally according to the miner's original timepiece system). The miner can modify the timestamp by a many seconds on the pledge that other miners accept the block they proposed. The vulnerability lies in the fact that some smart contracts take timestamp as a detector condition,e.g., transferring plutocrat, therefore adversary may manipulate the timestamp-dependent contracts for their own interests.

3) Mishandled Exceptions When a contract(frequenter) calls another contract(callee), if the callee runs abnormally, it terminates and returns false. This exception may or may not be passed to the frequenter. In principle, the frequenter must explicitly check the return value from the callee to corroborate that the call was executed successfully. still, If the frequenter doesn't duly check the return value, it'll bring implicit pitfalls. A typical case is the King of the Ether Throne contract in Ethereum.

4) Re-Entrancy Vulnerability When a contract calls another one, the current prosecution delays the call to finish. As the fallback medium allows a bushwhacker to re-up the frequenter function, the bushwhacker may use the intermediate state of the frequenter to conduct repeated calls, leading to circles of conjurations that recoup multiple refunds and clear the balance(12). The most notorious-entrance vulnerability is The DAO attack(21)

5) Callstack Depth Each time a contract invokes another, the call mound associated with the sale grows by one frame. The call mound is bounded to 1024 frames for Ethereum. When this limit is reached, a farther incantation throws an exception. An adversary starts by generating a nearly-full call mound, and also he or she invokes the victim's function, which will throw an exception. However, the adversary could manage to succeed in his/ her attack(22), If the exception isn't duly handled by the victim's contract.

3. Applications of Smart Contracts

Presently, operations for smart contracts are springing up. This section will take finance, operation, IoT, and energy as exemplifications to introduce the operation scripts of smart contracts.

A) Finance-

Blockchain and smart contracts enable increased visibility and trust across the actors while bringing huge savings in architectures, deals, and executive costs(36). The following are several typical operations of smart contracts in finance.

1. **Securities** - The security assiduity involves complex procedures that are time- consuming, bring hamstrung, clumsy, and prone to pitfalls. Smart contracts can circumvent interposers in the chain of securities guardianship and grease the automatic payment of tips, stock splits, and liability operation while reducing functional pitfalls. In addition, smart contracts can grease the clearing and agreement of securities. At present, major requests in the U.S., Canada, and Japan still have a 3- day agreement cycle(T 3)(37) that involves numerous institutions, similar as securities magazines and contributory operation agencies. The centralized clearing entails labor- ferocious conditioning and complex internal and external rapprochements. Blockchain enables bilateral peer- to- peer prosecution of clearing business sense using smart contracts. The Australian Securities Exchange is working on a DLT based post-trade platform to replace its equity agreement system(38).

2) **Insurances** - The insurance assiduity spends knockouts of millions of bones each time on recycling claims and loses millions of bones to fraudulent claims. Smart contracts can be exploited to automate claims processing, verification, and payment, therefore adding the speed of claim processing as well as barring fraud and precluding implicit risks(39). For illustration, The French airline, AXA, is taking flight insurance to smart contracts. However, they will get automatically notified of the compensation options, If passengers ' flight is further than two hours late. Smart contracts may also be used in bus insurance, because contracts can record the insurance clauses, driving records, and accident reports, allowing IoT- equipped vehicles to execute claims shortly after an accident.

3**) Trade Finance** - Trade finance is presently full of inefficiencies and the assiduity is extremely vulnerable to fraud. either, the paper- grounded processes of trade finance desperately need to be upgraded or replaced with digitalized operations. Smart contracts allow businesses to automatically spark marketable conduct grounded on predefined criteria that will boost effectiveness by streamlining processes and reducing both fraud and compliance costs. In July 2017, a trade sale was completed between Australia and Japan. This trade sale saw all the trade- related processes, from issuing a letter of credit to delivering trade documents completed entirely via the Hyperledger Fabric platform, which reduced the time needed to transmit documents, as well as the labor and other costs(40).

B) Management

Blockchain- enabled smart contracts can give applicable and transparent responsibility in terms of places, liabilities, and decision processes in operation. Some use cases follow.

1) **Digital parcels and Rights Management** - Storing cryptographic instrument of parcels or rights on blockchain can grease the access and confirmation. de la Rosa etal.(41) proposed to use smart contracts to certify the evidence of actuality and authorship of intellectual parcels. Propy allows possessors and brokers to register their real estate parcels, where buyers can search and negotiate the trade. Both parties share in the smart contracts together and specific way are taken throughout the process to insure fair and legal play. Smart contracts can also be applied in digital rights operation. For illustration, a DApp called Ujo Music apply the kingliness payments for a musician once his/ her work is used for marketable purposes.

2) **Organizational Management** - Now, utmost associations are managed by and centered on a board of directors who hold maturity of decision- making power. It's believed that the unborn organizational operation will be smoothed and decentralized. Smart contracts can remove gratuitous interposers that put artificial restrictions and unnecessarily complex regulations. For illustration, Aragon is a design powered by Ethereum that aims to disintermediate the creation and conservation of organizational structures, and empowers people across the world to fluently and securely manage their associations. In Aragon, commemoratives represent your stake in the association, you can use crowdfunding to raise finances encyclopedically and use voting for further effective results, you can also add a new hand to your association.

3) **E-Government** - Smart contracts can simplify regulatory processes and ameliorate the effectiveness and authority ofE-government. For illustration, Chancheng District in Foshan, China, established the firstE-government service platform using blockchain and smart contracts technology for the sake of perfecting the quality of government services, developing the individual credit system, strengthening the government's credibility, and promoting the integration of coffers(42). Other operation areas of smart contracts inE-Government include new payment systems for work and pensions, strengthening transnational aid systems,E-Voting(43),(44),etc.

C. IoT

IoT is an ecosystem of connected physical bias, vehicles, home appliances, and other particulars that are accessible through the Internet. IoT is believed to be extensively used in smart grids, smart homes, intelligent transportation, system, intelligent manufacturing, and other fields. The traditional centralized Internet system is delicate to meet IoT's development requirements, similar as the security of sensitive information and trusted commerce

between multi bias. thus, the combination of IoT and blockchain becomes an ineluctable tendency, and smart contracts will help to automate the complex workflow, promote resource sharing, save costs, and insure safety and effectiveness(45).

4. Future Scope

In this section, we will introduce the unborn development trends of smart contracts from three aspects, videlicet, formal verification, Subcaste 2, and smart contracts- driven resemblant organizational/ societal operation.

Formal Verification - Formal verification means applying a evidence that the program behaves according to a specification. In general, this is done with a concrete specification language used to describe how input and affair of functions are related. Formal verification of smart contracts involves proving that a contract program satisfies a formal specification of its geste (54). It corresponds to the operations subcaste in the exploration frame we proposed. The proposed model proved safety parcels of a smart contract using the interactive theorem provers(55). Amani etal.(54) extended an being EVM formalization in Isabelle/ HOL by a sound program sense at the position of bytecode. Hildenbrandt etal.(56) presented KEVM, an executable formal specification of the EVM bytecode mound- grounded language erected with the K Framework(57), which designed to serve as a solid foundation for farther formal analyses. Bhargavan etal.(8) outlined a frame to dissect and formally corroborate the functional correctness and runtime safety of Ethereum smart contract by rephrasing both reliability program and EVM bytecode utmost of these formal verification tools are still in the experimental stage and haven't been extensively used. In the future, formal verification will come an important exploration direction as it provides the loftiest position of confidence about the correct geste of smart contracts.