ScienceDirect

Future Generation Computer Systems

Volume 105, April 2020, Pages 475-491

An overview on smart contracts: Challenges, advances and platforms

Zibin Zheng [a], Shaoan Xie [a], Hong-Ning Dai [b], Weili Chen [a], Xiangping Chen [a], Jian Weng [c], Muhammad Imran [d]

Show more

Share Cite

https://doi.org/10.1016/j.future.2019.12.019

Get rights and content

Abstract

Smart contract technology is reshaping conventional industry and business processes. Being embedded in blockchains, smart contracts enable the contractual terms of an agreement to be enforced automatically without the intervention of a trusted third party. As a result, smart contracts can cut down administration and save services costs, improve the efficiency of business processes and reduce the risks. Although smart contracts are promising to drive the new wave of innovation in business processes, there are a number of challenges to be tackled. This paper presents a survey on smart contracts. We first introduce blockchains and smart contracts. We then present the challenges in smart contracts as well as recent technical advances. We also compare typical smart contract platforms and give a categorization of smart contract applications along with some representative examples.

Introduction

Blockchain technology has recently fueled extensive interests from both academia and industry. A blockchain is a distributed software system allowing transactions to be processed without the necessity of a trusted third party. As a result, business activities can be completed in an inexpensive and quick manner. Moreover, the immutability of blockchains also assures the distributed trust since it is nearly impossible to tamper any transactions stored in blockchains and all the historical transactions are auditable and traceable.

Blockchain technology is enabling *smart contracts* that were first proposed in 1990s by Nick Szabo[1]. In a smart contract, contract clauses written in computer programs will be automatically executed when predefined conditions are met. Smart contracts consisting of transactions are essentially stored, replicated and updated in distributed blockchains. In contrast, conventional contracts need to be completed by a trusted third party in a centralized manner consequently resulting in long execution time and extra cost.

The integration of blockchain technology with smart contracts will make the dream of a "*peer-to-peer market*" come true.

Take a smart contract between a buyer and a supplier as an example. As shown in Fig. 1, a supplier first sends a product catalog to a buyer through the blockchain network. This catalog that includes product descriptions (such as property, quantity, price and availability) along with shipping and payment terms is stored and distributed in the blockchain so that a buyer can obtain the product information and verify the authenticity and reputation of the supplier at the same time. The buyer then submits the order with the specified quantity and payment date via the blockchain. This whole procedure forms a purchase contract (*i.e.*, *Contract 1*) enclosed in the blue box as shown in Fig. 1. It is worth mentioning that the whole procedure is completed between the buyer and the supplier without the intervention of a third party.

After *Contract 1* is done, the supplier will search for a carrier in the blockchain to complete the shipping phase. Like *Contract 1*, the carrier also publishes the shipping description (such as transportation fees, source, destination, capacity and shipping time) as well as shipping conditions and terms in the blockchain. If the supplier accepts the contract issued by the carrier, the products will be delivered to the carrier who will finally dispatch the products to the buyer. This whole procedure constructs *Contract 2* (enclosed in the pink box) as shown inFig. 1. Similarly, the whole procedure of *Contract 2* is also conducted without the intervention of a third party.

In addition to automatic execution of *Contract 1* and *Contract 2*, the payment procedures (including the payment from the supplier to the carrier and that from the buyer to the supplier) are also completed automatically. For example, once the buyer confirms the reception of the products, the payment between the buyer and the supplier will be automatically triggered as the predefined condition is met. The financial settlement from the buyer to the supplier is conducted via crypto currencies (*e.g.*, Bitcoin or Ether.[1] .). In contrast to conventional transactions, the whole process is done in a peer-to-peer manner without the intervention of third parties like banks. As a result, the turnaround time and transactional cost can be greatly saved.

In summary, smart contracts have the following advantages compared with conventional contracts:

- *Reducing risks.* Due to the immutability of blockchains, smart contracts cannot be arbitrarily altered once they are issued. Moreover, all the transactions that are stored and duplicated throughout the whole distributed blockchain system are traceable and auditable. As a result, malicious behaviors like financial frauds can be greatly mitigated.
- *Cutting down administration and service costs.* Block-chains assure the trust of the whole system by distributed consensus mechanisms without going through a central broker or a mediator. Smart contracts stored in blockchains can be automatically triggered in a decentralized way. Consequently, the administration and services costs due to the intervention from the third party can be significantly saved.
- *Improving the efficiency of business processes.* The elimination of the dependence on the intermediary can significantly improve the efficiency of business process. Take the aforementioned supply-chain procedure as an example. The financial settlement will be automatically completed in a peer-to-peer manner once the predefined condition is met (*e.g.*, the buyer confirms the reception of the products). As a result, the turnaround time can be significantly reduced.

Smart contracts are boosting a broad spectrum of applications ranging from industrial Internet of Things to financial services [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]. Although smart contracts have great potentials to reshape conventional business procedures, there are a number of challenges to be solved. For example, even if blockchains can assure a certain anonymity of the parties of the contract, the privacy of the whole contract execution may not be preserved since all the transactions are globally available. Moreover, it is challenging to ensure the correctness of smart contracts due to vulnerabilities of computer programs to the faults and failures.

There are some recent studies on smart contracts. For example,[12], [13], [14] present comprehensive surveys of blockchain technology and briefly introduce smart contracts. The work of[15] provides an in-depth survey on Ethereum smart contract programming vulnerabilities while[17] presents a detailed survey over verification methods on smart contract languages. The work of[16] reports authors' experiences in teaching smart contract programming and summarizes several typical types of mistakes made by students. Ref.[18] presents an empirical analysis on smart contract platforms. Recent studies[19], [20] also collect some literature of smart contracts and present reviews while fail to discuss the challenges in this area. Moreover, the work of[21] presents a brief overview of smart contract platforms and architectures. However, most of existing papers fail to identify the rising challenges and give a comprehensive survey. For example, Ethereum can be used to conduct illegal business such as Ponzi schemes that were reported to defraud over 410,000 US dollars while few studies address this issue[22]. We summarize the differences between this paper and existing studies in Table2.

The objective of this paper is to conduct a systematic overview of technical challenges in smart contracts enabled by blockchain technologies. Contributions of this paper are highlighted as following:

- Important research challenges in the life cycle of smart contracts are identified.
- Recent advances in addressing technical challenges are summarized.
- A detailed comparison of typical smart contract platforms is made.
- Diverse smart contract applications are summarized.

Fig.2 shows the organization of this paper. In particular, Section2 gives a brief introduction to blockchains and smart contracts. Section3 then summarizes research challenges in smart contracts as well as recent technical advances. Section4 next compares typical smart contract development platforms. Section5 categorizes typical smart contract applications. Finally, Section6 concludes the paper.

Section snippets

Overview of blockchain and smart contract

Smart contracts are built upon blockchain technology ensuring the correct execution of the contracts. We first provide a brief introduction to blockchain technology in Section2.1. We then give an overview on smart contracts in Section2.2.

…

Challenges and advances of smart contract

Although a smart contract is a promising technology, there are still a number of challenges to be tackled. We categorize these major challenges into four types according to four phases of the life cycle of smart contracts. Meanwhile, we also give an overview on recent advances in solving these challenges. Table3 summarizes the challenges and recent advances.…

Smart contract development platforms

Recently, smart contracts have been developed on block-chain-based platforms. These platforms provide developers with simple interfaces to build smart contract applications. Among a number of incumbent blockchain platforms, many of them can support smart contracts. In this paper, we introduce 5 most representative smart contract platforms: Ethereum[89], Hyperledger Fabric[90], Corda[91], Stellar[92], Rootstock[93] in Section4.1. We choose them mainly due the popularity in developing…

Applications of smart contract

Smart contracts have a broad spectrum of applications ranging from Internet of Things to sharing economy. In particular, we roughly categorize major smart contract applications into six types as shown in Fig.8. We next describe them in details.…

Conclusion

This article presents an overview on the state-of-the-art of smart contracts. In particular, we first provide a brief review on smart contract and blockchain technologies. We then point out the challenges in smart contracts in different aspects of creation, deployment, execution, completion of smart contracts. Meanwhile, we also discuss the recent advances in solving these challenges. We next compare several major smart contract platforms. Moreover, we categorize smart contract applications and …

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.…

Acknowledgments

The work described in this paper was supported by the National Key Research and Development Program, China (2016-YFB1000101), the National Natural Science Foundation of China under (61472338) and the Fundamental Research Funds for the Central Universities, China. Imran's work is supported by the Deanship of Scientific Research at King Saud University, Saudi Arabia through the research group project number RG-1435-051. The authors would like to thank anonymous reviewers who have provided…

Zibin Zheng is a professor at Sun Yat-sen University, Guangzhou, China. He received Ph.D. degree from The Chinese University of Hong Kong in 2011. He received ACM SIGSOFT Distinguished Paper Award at ICSE'10, Best Student Paper Award at ICWS'10, and IBM Ph.D. Fellowship Award. His research interests include services computing, software engineering, and blockchain.…

Special issue articles Recommended articles

References (122)

YaqoobI. *et al.*
The rise of ransomware and emerging security challenges in the internet of things