Smart Contract Survey

Asma A. Alsufyani

Student in cyber security, Taif University, Taif 21944, Saudi Arabia

Email: AsmaAbbadSuf@gmail.com

Dr. Emad Alsuwat

Assistant Professor, Taif Universty, Saudi Arabia

Email: Alsuwat@tu.edu.sa

Abstract:

The smart contract supports a large number of contracts in various domains. It is an encrypted agreement to implement an exchange automatically when things are delivered, or services accomplished between two parties. It does not need for a third party to be an intermediary between the two parties to complete the contract, and it automatically executes agreement terms when the requirements are complete. It has many benefits such as autonomy, transparency, lower cost and efficiency. Smart contracts can build and implement in a public, decentralized and open source platform like Ethereum. Since it is a blockchain application, it is vulnerable to the blockchain vulnerabilities and some other specific attacks.

Keywords:

Security, Smart contract, Blockchain, Ethereum, Solidity

1. Introduction

Smart contract is an application of a Blockchain technology. Blockchain Technology is a growable and distributed list that contains sets of nodes, called blocks, which are connected with each other by a cryptography algorithm and separated over the Internet [1-3]. Blockchain concept has 6 major features: decentralized, transparent, open source, autonomy, immutable and anonymity. When we describe Blockchain as decentralized, we mean it has distributed blocks that do not need a third party to manage their operations. Transparent feature is a display of a public block for everyone. Open source characteristic means the blockchain network is open and avail-able for everyone to check and use. Blockchain is autonomy because each block must be approved by others to add to the Blockchain. Blockchain is immutable due to it being unalterable. Blocks identity is unknown, and this is a meaning of anonymity. Each block in Blockchain contains some types of data, like main data, called transaction, of the recent block and hashing of a prior block, hashing of transaction information, timestamp and nonce [1] [4].

As we mentioned, Smart contracts work in a Blockchain network. Smart contract is a digital and secure contract, that is executed between two parties directly without need to a third party [5]. We can also call smart contracts a self-executing contract because it is executed automatically [6] [7]. That no need for a third party or an intermediary lead to some benefits like the transactions will be more secure, faster, and cheaper than the traditional transactions. Transactions through a smart contract is more secure because it needs consensus which means that each transaction needs the agreement from all in a blockchain network to be accomplished, it is unchangeable, and it is anonymous. It is achieved using simple code under some conditions. We can use it for different reasons such as sell and pay, money transfers and exchange shares. Smart contract code is a simple program code, we can define it as a condition statement (if condition, then statement). To illustrate, if X payment of fees, then give X a receipt with an activation key to use it in a specific time. After implementing this code, it will decide what it should do [6].

The reminder of our paper proceeds according to the following structure. First, we present some works that are related to smart contracts. Next, we explain blockchain basics and the concept of smart contract. Then, we display the Ethereum platform. Finally, we show some smart contract attacks.

Study significance

We need to understand the smart contracts to be able to develop them, integrate them into other areas, and protect them against cyber threats. Therefore, we display the basic details of smart contracts in this paper to provide the knowledge base on the topic.

Study objectives

This paper is to display what is the smart contract, what are the main characteristics of it, what is the relationship between it and the blockchain, how does it work, and what are the threats to it. We aim to help researchers to understand this topic to develop its applications.

2. Related work

There are many works covered smart contract or used its concept to serve a specific goal, here we will display some of these works:

Jingqiu Gong,Shaofu Lin1 and Jingwen Li [8] suggested a model based on smart con-tracts to maintain the rights of personal health application data. The process of tracking and recording the source of personal health data, and who is generating it and "where" is called provenance, and this is the rights of the authors of this paper trying to protect it using smart contracts. Their suggested method consists of four phases: presentation the architecture of their model, data designed in the model, personal health data provenance function and use Rights confirmation and validation function. They found that their method is effective. Bogner, A., Chanson, M., and Meeuw [5] propose a decentralized application (DAPP) working through the Ethereum smart contract blockchain network. This application allows users to ex-change devices with each other without need to intermediary. DAPP solved the problems of the commune platforms of sharing stuff like rising prices and lack of privacy. P. McCorry, S. F. Shahandashti, and F. Hao [9] developed a self-execute vote protocol running through Ethereum smart contract. This protocol guarantees privacy for voters. Its implementation depends on the idea of consensus protocols on the blockchain network.

3. Blockchain and Smart contract

To understand the smart contract concept, we need to know the structure of the blockchain and how it works. Blockchain is a network of distributed and connected blocks. Each block in this network is made up of current transaction and hashing of a prior block, timestamp, hashing of current transaction information and nonce in a header of the block as illustrated in Fig. 1. Hash function used to make blocks unchangeable because it is a secure and unexpectable function [10]. The hashing of previous blocks is to relate the blocks with each other in the Blockchain network. Timestamp is to confirm the time when the block was created. Nonce is a unique number in each block used in the hash function [4]. Autonomy in

Blockchain achieved by using one of consensus protocols: proof of work protocol or proof of stack protocol. These two protocols specify the way of consensus, which is some predefined rules that used to decide if the new block can join to the Blockchain network or not. Merkle tree in blockchain used for making the varication process and the locomotion through the blocks faster [4].

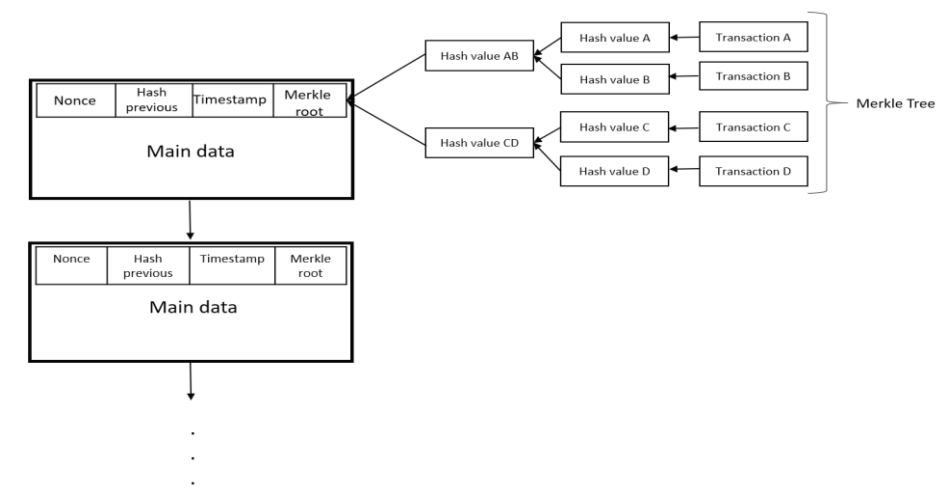

Figure 1.

Adapted from Asma A. Alsufyani [1], Arshdeep Bahga, Vijay K. Madisetti [3] and Iuon-Chang Lin and Tzu-Chun Liao [4].

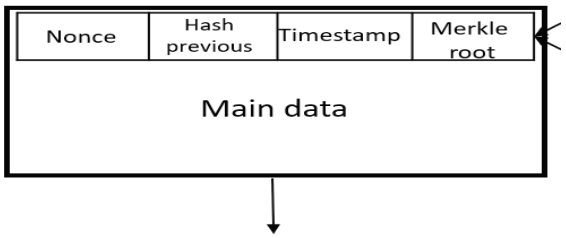

Figure 1a. Structure of block in Blockchain.

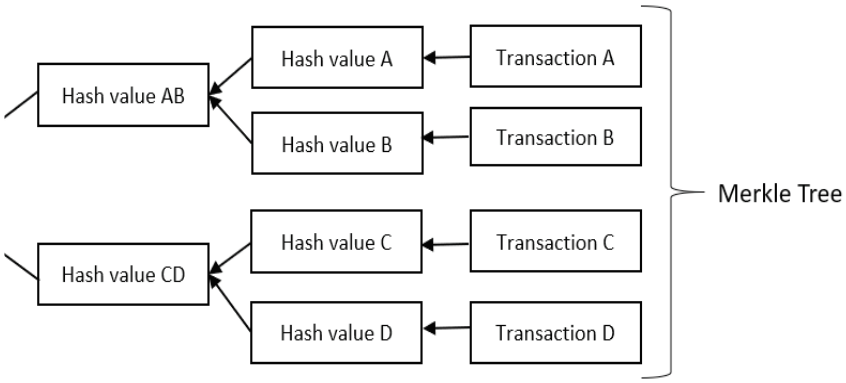

Figure 1b. Merkle Tree.

Smart contracts defined by Nick Szabo in the early 1990's [6]. It is a predefined program written by a user to determine specific conditions to carry out the contract after achieving them [6]. We can use it in insurance, mortgage loans, employment contracts, securing copyrighted contents and store information about an application. Smart contract has many advantages like saving time, money, and effort because it does not depend on a third party, unchangeable and transparent which makes it secure. It also has possible disadvantages like lack of regulations and humane errors. Humane error in programming is a drawback because the implementation of smart contract is automated after the contract joins a Blockchain network.

Ethereum is an open source and a global platform for decentralized applications. You can design a contract that deals with digital values, work precisely as programmed, and anyone around the world can access it on Ethereum platform [11].

It was designed in 2015 by Vitalik Buterin to allow people to build their own smart contract and distributed applications with their own rules. Transactions in smart contracts are called states and each state consists of accounts. Each account in Ethereum comprises: nonce, current ether balance, code and space for storage [7].

To execute the smart contract, we need "Ether" which is a digital cryptocurrency paid for computational resources that is used in the execution of the smart contract. We also need Gas to implement the computation process in the smart contract which is a tiny amount of the ether [12]. Gas is the fee needed to execute a transaction. Ethereum used solidity language to run its smart contracts. Solidity is a programming language designed to create and implement the smart contract through the blockchain. Figure 2 displays an example of solidity code. Externally owned accounts and contract accounts are two types of smart contract accounts in Ethereum. Private keys control the externally owned account, while a code that owned by the

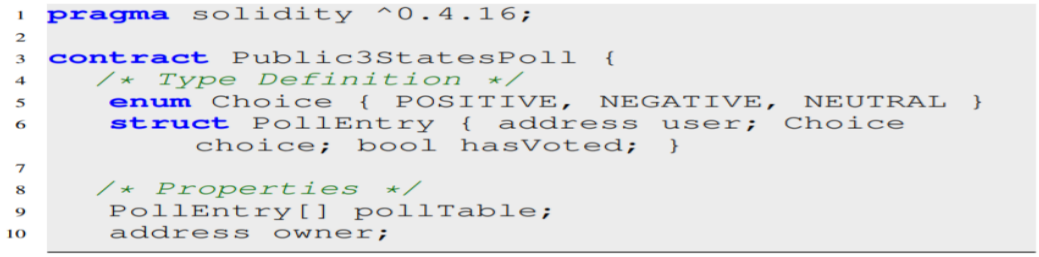

Figure 2. Adapted from Santiago Bragagnolo, Henrique Rocha, Marcus Denker, Stéphane Ducasse [14].

contract account has control of it. Both types of smart contract account have an ether balance. Nonce means the number that increases every time the account sends a transaction in an external account, while nonce in a contract account refers to the number that increases every time the account generates a new contract. Externally owned accounts send transactions to the contract account then the contract account performs these transactions [13] [14].

Smart Contract Attacks

Smart contract exposed to the same attacks of blockchain like 51% attack, fork issues, sybil attack and other [1] [4] [11]. It also exposed to other types of attacks like Ethereum smart contract attacks:

1. Decentralized Autonomous Organization (DAO)

Decentralized Autonomous Organization was distributed entities working over the Ethereum smart contract as a venture capital fund for the encipherment and dis-tributed space. It was allowed to anyone to fund using the ether. Shortly after its creation, it was hacked through the flaw in the DAO code. The attacker in this attack could steal money by sending multiple requests to a smart contract asking an ether, while the smart contract replies with ether to the first request and before it updates its balance the other request is come and steal. This was the end point of the DAO [15].

2. Rubixi

This attack designed to execute a pyramid scheme called Ponzi scheme, which is a fraudulent investing scam depends on a new investor to pay for the existing investor [15].

3. Multi-player games

The attacker in this type of attack takes advantage of a keeping secrets vulnerability. Keeping secrets vulnerable comes from the meaning of public contracts to all or even private contracts that will publish and disclose through the network of blockchain. The attacker impersonates the identity of one player from two player in the game and wins in any game he/she wants. The inspection of a transaction of the first players when the impersonator enters the game is the reason for this ability to win in any game [15].

4. Conclusion

Smart contracts proved its effect in many domains in the life of people. It was designed for many purposes like security, time and conflict saving and ease exchange compared to the traditional systems. In this paper We have presented an overview of the smart contract concept.

We display the blockchain characteristic to explain the smart contract, which is an application of blockchain. After that, we mentioned the smart contract plat-form: Ethereum. In the last, we give some examples of smart contract attacks.

5. References

[1] M. A. A. Asma A. Alsufyani, Ben Soh, Mehedi Masud, Jehad Al-Amri, "Application of Blockchain in Healthcare in Saudi Arabia," (in English), International Journal of Computer Science and Technology, vol. 11, no. 1, p. 7, 2020.

[2] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," F1000Research, vol. 5, 2016.

[3] M. A. AlZain, "Efficient Image Cipher using 2D Logistic Mapping and Singular Value Decomposition," INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, vol. 9, no. 11, pp. 196-200, 2018.

[4] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," IJ Network Security, vol. 19, no. 5, pp. 653-659, 2017.

[5] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the ethereum blockchain," in Proceedings of the 6th International Conference on the Internet of Things, 2016, pp. 177-178.

[6] R. R. W. H. G. Schulpen, "Smart contracts in the Netherlands- A legal research regarding the use of smart contracts within Dutch contract law and legal framework," Master, TILBURG UNIVERSITY, 2018.

[7] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.

[8] J. Gong, S. Lin, and J. Li, "Research on Personal Health Data Provenance and Right Confirmation with Smart Contract," in 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2019, vol. 1, pp. 1211- 1216: IEEE.

[9] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security, 2017, pp. 357-375: Springer.

[10] S. S. Gupta, Blockchain. John Wiley & Sons, Inc, 2017.

[11] N. Prusty, Building blockchain projects. Packt Publishing Ltd, 2017.

[12] C. Dannen, Introducing Ethereum and Solidity. Springer, 2017.

[13] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Rolebased access control using smart contract," Ieee Access, vol. 6, pp. 12240-12251, 2018.

[14] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, "SmartInspect: solidity smart contract inspector," in 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018, pp. 9-18: IEEE.

[15] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," IACR Cryptology ePrint archive, vol. 2016, p. 1007, 2016.