Smart Contracts: A Primer

Kelechi Eze
Prairie View A&M University
16 PUBLICATIONS 39 CITATIONS

Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2018, 5(5):538-541

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Smart Contracts: A Primer

Matthew N. O. Sadiku, Kelechi G. Eze, Sarhan M. Musa

Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446

Abstract A smart contract is a set of promises, specified in digital form, with a program enforcing the contract built into the code. Smart contracts run on blockchain technology, which is basically a distributed database that records all transactions that ever occurred in the network. A smart contract is an executable code that is executed on the blockchain to enforce an agreement between two or more parties. This paper provides a brief introduction to smart contracts.

Keywords smart contracts, blockchain contracts, digital contracts

Introduction

A contract is an agreement with obligations which are enforced by law. It is the basic building block of a free market economy. It is used in business, marriage, politics, etc. The digital revolution has brought new ways to formalize the relationships and contracts. The blockchain (literally, a "chain of blocks") has been introduced in 2008 as a digital technology that supports the verification, execution and recording of transactions between different parties. It is a novel solution to the age-old human problem of trust. A blockchain comprises a digital network and distributed ledger that track monetary transactions. It is a distributed database that records transactions in the network. It is regarded as a breakthrough technology that can benefit many sectors.

Using blockchain technology for smart contracts makes them tamper-proof, secure, transparent. A smart contract is a software program that adds layers of information onto the transactions being executed on a blockchain. Of all the five cryptocurrencies, the Ethereum is by far the most successful blockchain with smart contracts in mind. Although smart contracts can be encoded on any blockchain, Ethereum is mostly used [1].

The term "smart contracts" was coined in 1994 by American computer scientist Nick Szabo, who realized that the decentralized ledger could be used for smart contracts. Smart contracts are programmable contracts that are capable of automatically enforcing themselves when pre-defined conditions are met. A smart contract is an agreement between parties involved in a transaction that holds each party responsible. Smart contracts help in exchanging money, property, or any valuable thing in a transparent, conflict-free manner while avoiding the services of a middleman such a bank, a lawyer or a notary [2]. The relationship between traditional contracts and smart contracts is shown in Figure 1 [3].

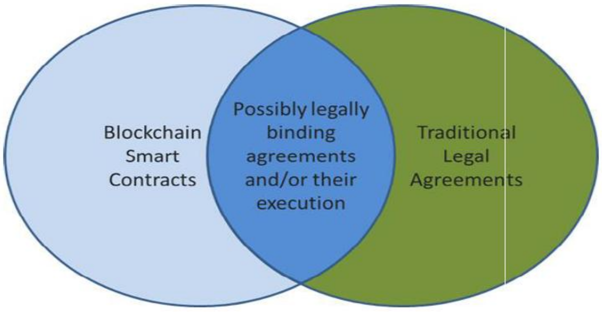
Blockchain Smart Contracts
Possibly legally binding agreements and/or their execution
Traditional Legal Agreements

Figure 1: Relationship between traditional contracts and smart contracts [3].

How Smart Contracts Work

A smart contract is a user-defined program running on top of a blockchain. Smart contracts allow the execution of credible transactions between mutually distrusting agents, without third parties. The major objective of smart contracts is to provide security that is superior to traditional contract law while reducing transaction cost. Smart contracts have features [4]: (1) solely electronic nature; (2) software implementation; (3) increased certainty; (4) conditional nature; (5) self-performance; (6) self-sufficiency. The smart contract system is illustrated in Figure 2 [5].

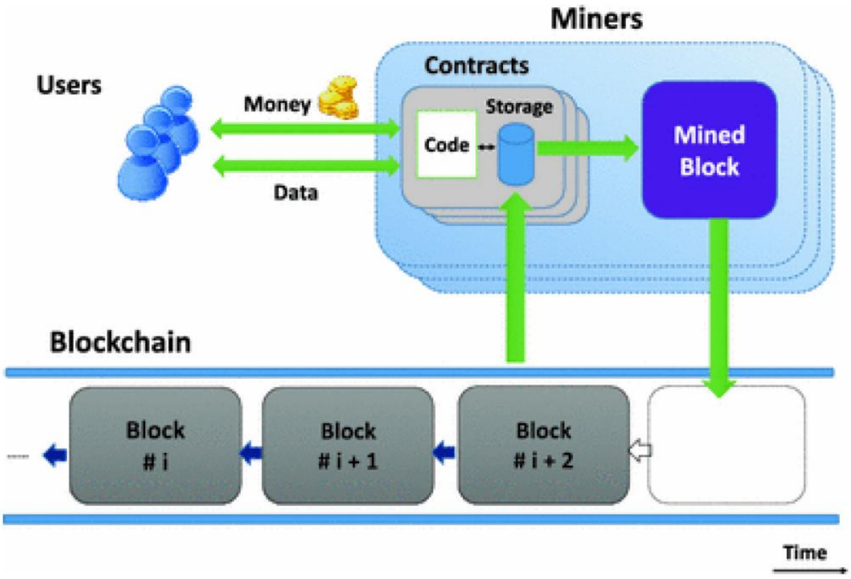

Figure 2: The smart contract system [5]

To deploy a smart contract in Ethereum, a special creation transaction is executed. This introduces a contract to the blockchain. During this procedure, the contract is assigned a unique address and its code is uploaded to the blockchain. Once successfully created, a smart contract is identified by a contract address [6]. The Ethereum address identity is assigned to every individual participating in the transaction. Each contract holds some amount of virtual coins and is associated with its predefined executable code. Cryptography plays a crucial role in this in that it is used for enforcement. The initiator of a transaction pays a fee (gas) for its execution, often measured in units of gas. Smart contracts automatically perform the contract terms according to the received information. The parties reach an agreement on the contents of the contract and perform the contracts according to the behaviors written in certain computer algorithms. Smart contracts are self-executable and self-verifying agents that cannot be changed once deployed in the blockchain.

Smart contract checks to see if participants in a transaction comply with the rules predefined in the smart contract. If they do, the transaction is validated; if not, the transaction is rejected [7]. Smart contracts can be used to transfer assets of considerable value. Hence, it is crucial that their implementation is secure and bug-free.

Applications

A Smart contract can be useful in a wide range of industries such as healthcare, automobiles, real estate, insurance, lotteries, supply-chain management, cryptocurrency exchanges, financial exchanges, covenants, law, government (e-voting system), creating a will, and many more [8].

- *Automobile:* For example, for self-parking vehicles, smart contracts could put into place a means of detecting who was at fault in a crash. Using smart contracts, an automobile insurance company could charge rates differently.
- *Real Estate:* For example, rent your apartment to someone, and the ledger cuts your costs. All you do is pay via bitcoin and encode your contract on the ledger. You accomplish automatic fulfilment.

- *Healthcare*: Personal health records could be encoded and stored on the blockchain. The ledger can be used for healthcare management, such as supervising drugs, regulation compliance, and managing healthcare supplies.

Benefits and Challenges

The key characteristic of a smart contract is that its contents cannot be manipulated, and its execution cannot be prevented. A smart contract cuts out discrepancies that typically occur with tradition contract processing which may lead to costly lawsuits. Blockchain is not just about eliminating the middleman. Blockchain could disrupt markets and drives cost savings by reducing labor-intensive processes and eliminating duplicate effort. Its transparency, security, and efficiency make it a particularly good choice for reshaping businesses [9]. Smart contracts are disintermediated and anonymous transaction. They offer the promise of increased commercial efficiency, lower transaction and legal costs. They may eliminate human bias and reduce the need for lawyers.

Smart contracts are not immune from errors, omissions, or fault. The technology has yet to be fully developed, meaning that the spectrum of possible applications has not been fully explored. Ethereum (launched officially in June 2015) and the security of its smart contracts are in their infancy stage.

Smart contracts can handle hold millions of dollars, easily making financial incentives high enough to attract adversaries. Their correct execution is crucial against attackers who may want to steal the assets. Writing secure smart contracts can be very difficult due to the open nature of Ethereum.

Conclusion

The programs designed to run on the Ethereum platform are commonly referred to as smart contracts. A smart contract is a computerized transaction protocol that executes the terms of a contract. It may be regarded as a computer program that regulates and automates the relationship between two or more non-trusting parties. It is a specific application of blockchain technology.

Smart contracts are receiving increasing attention in business, science, government, and academia because they eliminate the need for a trusted third party. The introduction of smart contract has caused some disruption in the contract market.

References

[1]. "Smart Contracts and the Blockchain, Explained," https://www.fool.com/investing/2018/03/09/smart-contracts-and-the-blockchain-explained.aspx

[2]. N. Szabo, "Smart contracts: Building blocks for digital markets," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[3]. "Smart contracts as a specific application of blockchain technology," https://blockchaingers.org/posts/smart-contracts-as-specific-application-of-blockch

[4]. A. Savelyev, "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law," *Information & Communications Technology Law*, vol. 26, no. 2, 2017, pp 116-134.

[5]. K. Delmolino et al., "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," *Proceedings of the International Conference on Financial Cryptography and Data Security*, Springer 2016, pp. 79-94.

[6]. M. Wöhrer and U. Zdun, "Smart contracts: Security patterns in the Ethereum ecosystem and solidity," *Proceedings of the International Workshop on Blockchain Oriented Software Engineering*, 2018, pp. 2-8.

[7]. V. Shermin, "Disrupting governance with blockchains and smart contracts," *Strategic Change*, vol. 26, no. 5, 2017, pp. 499–509.

[8]. A. Rosic, "Smart contracts: The blockchain technology that Will replace lawyers," https://blockgeeks.com/guides/smart-contracts/

[9]. P. Sreehari et al., “SMART WILL converting the legal testament into a smart contract,” *Proceedings of the International Conference on Networks & Advances in Computational Technologies*, July 2017, pp. 203-207.

About the Authors

Matthew N.O. Sadiku (sadiku@iee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is an IEEE fellow. His research interests include computational electromagnetics and computer networks.

Kelechi G. Eze (keze@student.pvamu.edu) is a doctoral student at Prairie View A&M University, Texas. He is a student member of IEEE. His research interests include Internet of things security, data security and privacy, blockchain technology, wireless sensor networks, and machine learning.

Sarhan M. Musa (smmusa@pvamu.edu) is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow.