International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Smart Contract Development, Adoption and Challenges: The Powered Blockchain

Husneara Sheikh[1], Rahima Meer Azmathullah[2], Faiza Rizwan[3]
[1, 2, 3]Computer Science, Prince Sattam Bin Abdalaziz University, Wadi Addawasir, Riyadh, Saudi Arabia, 19911
Email address: [1]h.sheikh@psau.edu.sa; [2]a.rahima@psau.edu.sa, [3]r.faiza@psau.edu.sa

Abstract-- *The purpose of this paper is to understand smart contracts, its benefits over traditional agreements and technical explanation about its execution and deployment. We have highlighted its origin, characteristics and adoption among different industries and its purpose in the blockchain world. We will also discuss the significant mechanism and their communication for the Blockchain and Ethereum to work. This paper will also explain about concepts of Blockchain and Ethereum in brief for scripting Solidity contracts. Finally, we conclude the discussion with its benefits and hypothesis.*

Keywords-- *Blockchain; Ethereum; Smart Contract; Use Case.*

I. Introduction To Smart Contract

The term *smart contract* appeared over twenty years ago and has emerged with blockchain technology. This concept and idea of implementation and saving smart contracts in a distributed ledger has been offered by Nick Szabo, a cryptographer. The innovation and impact of technology from IoT to AI to Blockchain has already taken over many industries. The application of blockchain have achieved tremendous force in terms of decentralized and immutable distributed databases for few years.

II. Smart Contract Definition

What are smart contracts?

Smart contracts are programming code which stored on blockchain and automatically execute when predetermined and programmed terms and conditions are met. The advantages of smart contracts are mostly required for business relationships where it is used as an agreement between the business alliances so that they can rely on consequences without involving any intermediary.

A smart contract is a legal contract between two parties in the form of programming code. The programmed agreement is unaltered and stored on distributed database which executes on the blockchain. All the transactions of the smart contract are processed by the blockchain when the conditions in the agreement are matched as there is no intermediary involved.

III. Smart Contract Explanation

A. History/Origin

Nick Szabo, a cryptographer originated with an idea of recording contracts in a coding form in the year 1994. This pre-defined the contract is a set of rules that executed automatically if the conditions are matched without involvement of any intermediary. Smart contracts are developed on many different blockchain platforms like Ethereum. It is a simple decentralized mechanism. The pre-defined code simplifies, authenticates, and implements the performance of an agreement or transaction.

B. Simple Explanation

i. What do Smart Contract do?

Smart contracts can simplify the complex and tedious process of any transaction which requires more paper work to identify the credentials of a person. The blockchain technology can make transactions secure and solidify as it stores all the personal information for verification and reduces the repetitive task to make quick decision for the customer. The smart contract is a coded agreement to be made between the bank, seller or dealer and the buyer or lender. The transactions declared completed once the seller receives the payment from the buyer and the buyer hold the item based on the agreed terms and conditions. The smart contract executed automatically without interference of any third party and makes the transaction reliable. The transaction is recorded in blockchain as it is shared between the participants and can be viewed at any time.

This mechanism comprises of digital assets and the participating parties who deposit assets into the smart contract. The digital assets are then redistributed to all the participant parties as per the built formula based on the definite data, unknown during the commencement of the contract.

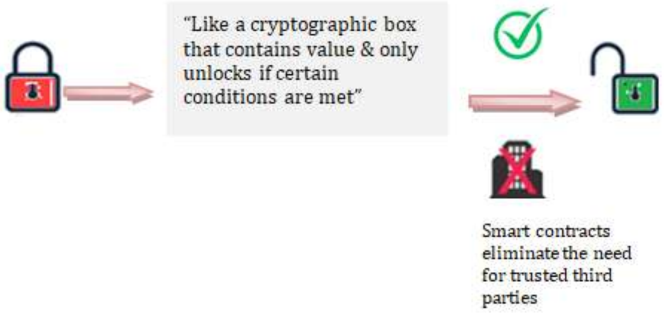
"Like a cryptographic box that contains value & only unlocks if certain conditions are met"
Smart contracts eliminate the need for trusted third parties

Fig. 1. Smart contract mechanism

The smart contract should not be confused with legal contracts agreed by law or courts. This can only be fully implemented in few years if they rely on its emerged technology and if the legal standards are approved.

ii. Characteristics of a Smart Contract

Smart contracts are used to track real-time performance and can save huge costs. Smart contracts have information oracles so that it can extract external information. They are immutable, auto-executing and possess self-validating features.

iii. Benefits of Smart Contract

The benefits of smart contracts works together with blockchain,

- Fast and Precise: Smart contracts are easily processing a computer-coded and pre-defined agreement which has replaced tremendous paper work documentation and miscalculations.
- Reliable: Smart contracts have pre-determined rules in which the whole transaction executes automatically. The transaction records are immutable, secured and distributed among the parties involved in the process.
- Secured: The smart contracts are more secure as they work on blockchain technology where all transactions are linked with the previous and successive records on a distributed ledger.
- Savings: Smart contracts avoid third parties as parties can rely on data and technology for correct execution of the transaction. It does not require any intermediary for verification and validation for the terms and agreement as it is already in coded form.

The benefits that make smart contracts differ from traditional contracts for businesses are:

- Direct communications with consumers. A smart contract avoids intermediaries and allows apparent, direct interactions with customers.
- No loss of data: As there is no intermediary between the transactions, blockchain technology offers decentralization where it protects the data in the network and accessible for the authorized consumer.
- Trustworthy. The business agreements are unchangeable and indestructible as these are executed automatically in case of smart contracts.
- Fraud declination. Smart contract transactions are verified by the parties in the network as it is saved in distributed blockchain network. Therefore, smart contract data cannot be changed by anyone as other participants can find and make it an invalid transaction.
- Cost effectiveness. It can avoid additional charges as there are no intermediaries involved where business people and consumers can interact directly for every transaction.
- Record protection. Smart contract transactions are kept in sequential order in the blockchain and can be retrieved along with the whole audit stream.

iv. Smart Contract Benefits for Business

Direct Dealing with customers	Resistance to failure	Immutability
Fraud reduction	Cost efficiency	Records Keeping

Fig. 2. Smart Contract benefits for business

v. Why trust a Smart Contract?

Smart contracts are possessed with the properties of blockchain as they are designed and implemented with the blockchain technology.

C. *Technical Explanation*

i. How to write Smart Contract?

Though there are many smart contract authoring tools available, however, Remix is a quick and easy browser based tool used to Develop smart contract It provides IDE for all the process including authoring and deployment are carried out from the same environment.

ii. How the contracts are deployed

Compilation of contract is the initial step to develop smart contracts with the help of solidity compiler. Compiler creates two important objects: Application Binary Interface (ABI) definition and Contract byte code.

ABI is required for invoking functions in the contract. It is an interface consists of external and public function declarations with their parameters and return types. The ABI defines and generate a new instance for the contract and can be used if any caller calls the contract function.

The bytecode required for deployment process, it characterizes the contract and deployed in Ethereum network. When ABI definition generates a new instance for the contract which creates a new transaction that can be mined. After mining the transaction, the contract is accessible at an address firmed by Ethereum. Once the contract is deployed in Ethereum Virtual Machine, the contract and the functions can be invoked with the help of recently created address.

IV. TRADITIONAL VS SMART CONTRACT

What is a contract

A contract is a legal file or document implemented by the law which connects different parties for an agreement agreed to be performed in future. Upon a common deal to be execute a transaction immediately or in future like business partnership or property dealings.

On the other hand, a smart contract is a coded form of legal contract which is applied, organized, saved and executed within the Ethereum Virtual machine environment. The data reside in the smart contract are used to record any kind of information required to work for the legal industrial contracts. The functionality is just like the object oriented programming where the smart contract call another smart contract and their functions. As object is created as an instance for the class, the instance of the smart contract is created and it can invoke other functions to perform or execute some logic.

V. HOW DOES SMART CONTRACT WORK?

Smart contracts functions based on common "If" statements coded on blockchain where the systems on the network perform or execute the events like monetary dealings, registration of certificates, renewing of license, etc. These transactions are executed when the coded contract is matched with legal agreement. When the transaction finishes its execution with perfection then it updates the blockchain. In order to achieve the satisfied transaction, the parties to a blockchain platform have to conclude whether the transactions and data are landed on the administered policies and describes structure to solve disagreements.

Smart Contracts can:

- Change legal contracts into automated procedures.
- Assure high security.
- Diminish intermediary reliance.
- Low transaction charges.
- Save information about an application.
- It gives utility to other contracts as a software library does.

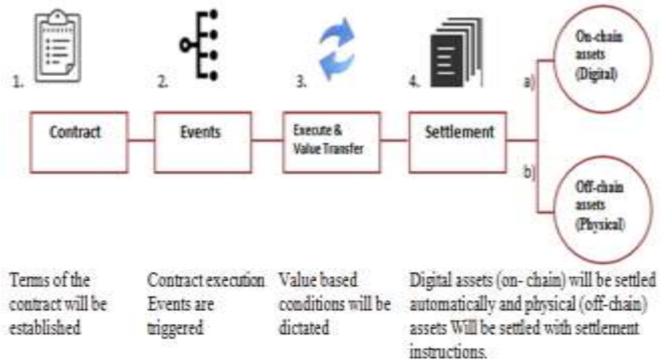
1.
2.
3.
4.
Contract
Events
Execute & Value Transfer
Settlement
a)
b)
On-chain assets (Digital)
Off-chain assets (Physical)
Terms of the contract will be established
Contract execution Events are triggered
Value based conditions will be dictated
Digital assets (on- chain) will be settled automatically and physical (off-chain) assets Will be settled with settlement instructions.

Fig. 3 Step-by-step process of smart contract execution

Initially bitcoin maintained and validated smart contract transaction after the conditions were met. Later on, Ethereum substituted bitcoin scripting language with other programming languages. The programmers can develop their own smart contracts with the help of Ethereum.

D. How does Blockchain Smart Contract work?

Smart contract basics

A blockchain is a digital network constructed and retained by the software executing within distributed computers. Blockchain uses cryptocurrencies and consists of digital and distributed the ledger that measures and stores financial transaction.

Blockchain are more faster and accurate than the traditional ledger as it is decentralized technology used for digital transactions. In this case, the smart contract builds a trust for digital transactions which runs within blockchain network. It processes composite transaction with speed and accuracy. That is where, it helps the smart contract where the participated parties are responsible for their transactions.

E. How does Ethereum Smart Contract Work?

As mentioned in the introduction, the cryptographer Nick Szabo has designed and planned about the vending machine where user can enter value and retrieves required thing from a device. Here, actually the contract is made where user can enter the data which execute and provide desired results. Ethereum is one of the platforms where the smart contract can be developed.

VI. SMART CONTRACT USE CASES

Smart contracts are getting advanced and has been operated in different blockchain projects. Following are the various potential Here are just several promising examples of smart contract implementations in different sectors.

Banking

Banking is the most promising industry where smart contracts is implemented over traditional transaction such as loan payment and other financial operations which allows customers for automatic smart checks and digital attestation.

Healthcare

Smart contracts can work better in healthcare sector. They can simplify various operations such as information retrieval, patient confidentiality, data confirmation and approval. Encrypgen is an application which is used to securely transfer patient information without any intermediary. It is up to the patient if they want to share their data as per their wish.

Supply Chain and Business Management

Supply chain is the another sector where the smart contract confirms smooth tracking for inventory and goods. It also minimizes fraud threat. Smart contracts are operated efficiently in various marketplaces.

Smart contracts has also been promoted in business management in terms of automated employee payroll system.

Legal Issues and Real Estate

Smart contracts are worked incredibly for determining legal issues as it provides automated and neutral clarification over traditional certification of documents and notarization. This technology has positive impact on real-estate projects too to solve many complex and widespread problems.

Government

The most promising impact of smart contract decentralization is on government systems such as voting system. The blockchain based voting system provides secure, inexpensive various voting operations. The main factor for the smart contract based voting system is to facilitate apparent and impartial voting all over the world. There are applications like 'FollowMyVote' operates on smart contract and blockchain technology to secure voting information. The voting information is immutable once it is printed on blockchain network.

The Internet of Things Networks

Smart contracts can also join with other technologies like Internet of Things where both can together control considerable changes among various industries. For example, the project named "Oaken" offers independent IoT hardware and software joined with blockchain technology to operate on different real-time requirements.

VII. CHALLENGES AND HYPOTHESIS

We have all understood the mechanism of smart contract technology which has eliminated the third-party member for monetary transaction, property assets or any valuable dealings. Though it has ample of benefits, however, it can also be created unknown confusion as small failure can cause incredible losses. It is still hypothetical whether the technology can provide more benefits as expected and implemented. There are few projects which experienced problems to be resolved. Moreover, market investors and business people need to have complete knowledge about the technicalities and compatibilities of the smart contract and digital currencies that work on blockchain.

VIII. CONCLUSION

Smart contracts promote and create a favorable and trustworthy business association contrasting to the traditional business representation. Smart contracts provide unchangeable distributed storage system for legal agreements that derived from blockchain properties. This property makes the business sector incredibly reliable on financial and legal transactions. Though it is difficult to implement this incredible technology to revolutionize industries and it would take significant amount of time and effort, however, flourishing use cases for the blockchain and smart contract technologies are creating a promising business prospect.

REFERENCES

[1] BitDegree Tutorials, "What is Smart Contract and How does it work?", by Ray King, 1992. https://www.bitdegree.org/tutorials/what-is-a-smart-contract/

[2] Coinmonks**,** **"**Introduction to Blockchain, Ethereum and Smart Contracts—Chapter 1", by Ritesh Modi, 2018. https://medium.com/coinmonks/https-medium-com-ritesh-modi-solidity-chapter1-63dfaff08a11

[3] RubyGarage, "A Guide to Smart Contracts and Their Implementation", by Tania H., 2018, https://rubygarage.org/blog/guide-to-smart-contracts

[4] IBM, "What are Smart Contracts on Blockchain" by Nigel Gopie, 2018, https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/

[5] BlockchainHub, "Smart Contracts", https://blockchainhub.net/smart-contracts/

[6] Coindesk, "How Do Ethereum Smart Contracts Work?", https://www.coindesk.com/information/ethereum-smart-contracts-work

[7] The Mottely Fool, "Smart Contracts and the Blockchain, Explained ", by Maxx Chatslo, 2018. https://www.fool.com/investing/2018/03/09/smart-contracts-and-the-blockchain-explained.aspx

[8] Forbes, "Blockchain Smart Contracts: More Trouble Than They Are Worth?", by Shermann Lee, 2018. https://www.forbes.com/sites/shermanlee/2018/07/10/blockchain-smart-contracts-more-trouble-than-they-are-worth/#41901c3d23a6