ALL YOU NEED TO KNOW ABOUT BLOCKCHAIN SMART CONTRACTS

Swathi Shreeramkumar,

Student, Alliance university, school of law, Bangalore, Karnataka, India

ABSTRACT:

The most attractive feature of blockchain technology is the SMART CONTRACTS. A smart contract is an executable code that runs on top of the blockchain to facilitate, execute and enforce the terms of an agreement between the untrusted parties without the interference of the trusted third party.[1] In current systems, the transactions are usually conducted in the presence of the trusted third party which is a centralized manner resulting in security issues and high monetary transaction fees. The most relevant example of such contracts are banking transactions. Introduction of the blockchain technology has enabled to tackle the above said issues by allowing the untrusted parties to interact with each other without the interference of the trusted third party in a distributed manner. Blockchain is a distributed and decentralized networking database that keeps a record of all the transactions that has ever happened in the network. It was originally introduced for bitcoin which is a peer to peer digital payment system but evolved to be used for the development of wide range of decentralized applications. The important advantages of these contracts are that they are cost effective and avoid the interference of third party promoting confidentiality and security. This paper explains the basics of blockchain technology, smart contracts, relevant platforms that can be utilized to create smart contracts, application of smart contracts and various issues related to these contracts.

KEYWORDS: *Blockchain, smart contracts, digital contracts, technology*

INTRODUCTION:

A smart contract is an executable code that runs on top of the blockchain to facilitate, execute and enforce the terms of an agreement between the untrusted parties without the interference of the trusted third party.[2] Introduction of the blockchain technology has enabled to tackle the security issues and high monetary transaction fees by allowing the untrusted parties to interact with each other without the interference of the trusted third party in a distributed manner. Blockchain is a distributed and decentralized networking database that keeps a record of all the transactions that has ever happened in the network. It was originally introduced for *bitcoin* which is a peer to peer digital payment system but evolved to be used for the development of wide range of decentralized applications. The important advantages of these contracts are that they are cost effective and avoid the interference of third party promoting confidentiality and security.

BLOCKCHAIN:

Blockchain is a distributed and decentralized networking database that keeps a record of all the transactions that has ever happened in the network. It was originally introduced for *bitcoin* which is a peer to peer digital payment system but evolved to be used for the development of wide range of decentralized applications. This database is replicated and be accessed by various participants of the network. The most important feature of this technology is that it provides for the secure and confidential communication and transaction by the untrusted parties by themselves without the interference of the trusted third party, thus enabling confidentiality and security. The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to

[1] Buterin,V. (2017/02/19) A next generation smart contract and decentralized application platform. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper

[2] Buterin,V. (2017/02/19) A next generation smart contract and decentralized application platform. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper

record not just financial transactions but virtually everything of value.[3] Blockchain is an ordered list of blocks, where each block is identified by its cryptographic hash.

Each block references the block that came before it, resulting in a chain of blocks. Each block consists of a set of transactions. Once a block is created and appended to the blockchain, the transactions in that block cannot be changed or reverted. This is to ensure the integrity of the transactions and to prevent double-spending problem. Cryptocurrencies have emerged as the first generation of blockchain technology. Cryptocurrencies are basically digital currencies that are based on cryptographic techniques and peer-to-peer network. The first and most popular example of cryptocurrencies is Bitcoin. Bitcoin is an electronic payment system that allows two untrusted parties to transact the digital money with each other in a secure manner without going through a third party (e.g., a bank).[4] Transactions that occurred in the network are verified by special nodes called miners. Verifying a transaction means checking the sender and the content of the transaction. Miners generate a new block of transactions after solving a mathematical puzzle which is called Proof of Work and then propagate that block to the database. Other nodes in the network can validate the correctness of the generated block and build upon it only if it was generated correctly. However, Bitcoin has limited programming capabilities to support complex transactions. Bitcoin does not support the creation of complex distributed applications. Other blockchains such as Ethereum have emerged as the second generation of blockchain to allow building complex distributed applications beyond the cryptocurrencies. Smart contracts, which will be discussed in the following section, are considered as the main element of this generation.[5] Ethereum blockchain is the most popular blockchain for developing smart contracts. Ethereum is a public blockchain with a built-in Turing-complete language to allow writing any smart contract and decentralised application.[6]

SMART CONTRACTS:

A smart contract is a contract in which the terms and conditions of that agreement are codified in a software. A smart contract is an executable code that is found in the blockchain networks which facilitates, executes and enforces the terms of any agreement between the untrusted parties. The primary aim of the smart contracts is to execute and enforce the terms of the agreement once the specified conditions and validities are duly met. Thus, smart contracts are cost efficient compared to those traditional contracts. These contracts are difficult to erase or change enabling a clear trail of audit. The idea of smart contracts came from Szabo in 1994. However, the idea was established after the emergence of blockchain technology. A smart contract can be thought of as a system that releases digital assets to all or some of the involved parties once arbitrary pre-defined rules have been met.[7] The obligations of the contract are strictly coded that if any changes or amendments are made, the terms of the agreement shall be enforced from the beginning again. For instance, Alice sends X currency units to Bob, if she receives Y currency units from Carl. There exists a difference between smart contract code and smart legal contract. The smart code that is verified, stored and executed on the blockchain network is called a smart contract code. The capability of this code depends on the programming language that is used to express the terms of the contract. The code that is used to complete or substitute other legal contracts are called smart legal contracts. The capability of smart contracts does not depend on the technology but the legal, business and political institutions. Smart contract consists of three parts: an account balance, a private storage and an executable code. There are two types of smart contracts: deterministic and non-deterministic smart contracts. A deterministic smart contract is a smart contract that when it is run, it does not require any external information from outside the blockchain. On the other hand, a non-deterministic smart contract depends on the information called oracles or data feeds from the external party. For example: a contract that requires

[3] Don & Alex Tapscott, (2016) Blockchain Revolution. Retrieved from https://blockgeeks.com/guides/what-is-blockchain-technology/

[4] Nakamoto,S. (2008) bitcoin: A peer to peer electronic cash system.

[5] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen,(2016) "The blockchain as a software connector," in 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)

[6] Alharby, Maher & van Moorsel, Aad. (2017). *Blockchain Based Smart Contracts: A Systematic Mapping Study*. Retrieved from: https://www.researchgate.net/publication/319603816_Blockchain_Based_Smart_Contracts_A_Systematic_Mapping_Study

[7] Buterin,V. (2017/02/19) A next generation smart contract and decentralized application platform. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper

information regarding weather or climatic conditions is a non-deterministic smart contract as these information is not available on the blockchain.

PLATFORMS FOR SMART CONTRACTS:

There are various blockchain platforms that provide for the development and deployment of smart contracts. Different platforms provide different features for the development of smart contracts. High level programming languages are supported by few platforms. The most popular platforms are *BITCOIN, ETHEREUM and NXT.*

BITCOIN is a public blockchain platform that can be used to process and transact cryptocurrencies. But they provide for a very limited commute capability.

ETHEREUM is a public blockchain platform that supports advanced and customizable smart contracts with withdrawal limits, loops, financial contracts and gambling markets.

NXT is a public blockchain platform that includes built-in smart contracts as templates.

APPLICATIONS OF SMART CONTRACTS:

There are various usages of smart contracts. A few of them are listed below:

1. E-voting
2. Motor insurance
3. Mortgage payments
4. Right management through digital technology
5. Identity management
6. Supply chain
7. Distributed file storage
8. E-commerce
9. Music rights management
10. Smart property
11. Internet of things
12. Anti-money laundering (AML) and Know Your Customer (KYC)
13. Stock trading
14. Land title registration
15. Neighbourhood microgrids

LEGAL REGULATIONS OF SMART CONTRACTS:

REGULATIONS OF SMART CONTRACTS AROUND THE WORLD:

The basic valid essentials of a valid contract shall be fulfilled by smart contracts. Those valid essentials are: valid offer, valid acceptance, lawful subject matter and consideration, valid consent and competency of the parties. UNIFORM ELECTRONIC TRANSACTIONS ACT (UETA) was adopted by around 47 states in the United States of America (USA) in 1999. This act regulates the transactions like electronic contracts and regulations regarding such contracts, records and signatures. The act also recognized electronic or digital signature as a valid form of consenting to the terms of the contract. In 2017, special regulations with regards to the recognition of signatures provided for smart contracts and giving evidentiary value to the smart contracts if any dispute arises were made by various states such as Arizona[8], Vermont and Nevada[9] etc.,

[8] Article 5, HB 2417, State of Arizona, 53rd Legislature, 2017, available at: http://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf

[9] [2] Senate Bill No. 398, State of Nevada, March 20, 2017, available at: https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB398_R1.pdf; *See also,* Act No. 157 (H. 868), House Committee on Commerce and Economic Development, State of Vermont, 2017, available

REGULATIONS OF SMART CONTRACTS IN INDIA:

In India, smart contracts are regulated through the INFORMATION TECHNOLOGY(IT) ACT of 2000. Section 5 of the IT act allows the contracts and records to be validated using electronic or digital signatures.

Section 5 of the IT Act:

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his handwritten signature or any mark on any document and the expression "signature" shall be construed accordingly. [10]

Chapter VII Of the IT Act covers various aspects of the digital signature certificates. Section 35 provides that the digital signature shall be obtained only from the government designated certifying authority. Section 36 provides for the representations and condition s to be complied with for the issuance of digital signatures. The provisions for the suspension and revocation of digital signatures are covered under sections 37 and 38 respectively.

Various amendments have been made to the INDIAN EVIDENCE ACT, 1872 on order to include provisions for the admissibility of electronic agreements, records and signatures.

85B. Presumption as to electronic records and [electronic signatures]. —

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that— (a) the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record; (b) except in the case of a secure electronic record or a secure [electronic signature], nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any [electronic signature].[11]

Thus, for a smart contract to have evidentiary value according to Indian Evidence Act, 1872, it has comply with the conditions provided in the IT Act, 2000.

CONCLUSION:

Considering the above said explanation, it's a revolutionary and a modern evolution if smart contracts are adopted in various fields. There are various disadvantages and technical issues in using smart contracts such as codifying and security issues and privacy and performance issues. The legal implications must also be kept in consideration before the execution of smart contracts. A wide scale adoption of technology would require the government to make amendments to the Information Technology Act, 2000 and the Indian Evidence Act, 1872, if specific regulations are not made. Thus, I conclude that adoption of smart contracts would be effective only after the issues are identified and rectified and appropriate laws are made or amended to regulate the hassle free usage of such contracts.

---

at: http://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20Act%20Summary.pdf

[10] Section 5 of the Information Technology Act,2000

[11] Section 85B of the Indian Evidence Act, 1872 Subs by Act 10 of 2009, s. 52(e), for —digital signature‖ (w.e.f. 27-10-2009).