Blockchain Technology and Smart Contract

Blockchain

Blockchain is a decentralized, distributed, and transparent collection of the ledger. Millions of computers as in nodes comprises a Blockchain Network, the term generally associated with financial transaction caught researchers attention for the first time from Satoshi Nakamoto's work on Bitcoin. [1] Blockchain's first application is Bitcoin, a digital cryptocurrency [1]. Its unique characteristics made it reliable for online transactions, as well as a reliable record keeper of other kinds of information.

In a Blockchain network, each node or user computer contains a copy of the Blockchain. That implies millions of copies of the identical ledger are stored in millions of computers in the network concurrently. In a Blockchain architecture, each block's contained information is visible to all users. This visibility to the user conforms to the transparency of the system. These unique characteristics of distributed ledgers to all over the network makes Blockchain somewhat immune to attack. It's next to impossible to override the majority of the blocks without being unnoticed. This level of immunity conforms to the security of the transaction. Blockchain's thousands of bytes of information aren't stored in a central database, rather stored in each node of the Blockchain network. This decentralized character makes the Blockchain, a system with no regulatory body. Its transactions are validated by its computers on the network at that time. Computers perform a mathematical operation of high complexity to validate transactions and add blocks in the chain. Incentives in cryptocurrencies are common for this labor.

Types of Blockchain:

Blockchain is a distributed ledger technology (DLTs) [2]. Blockchain is secure compared to traditional maintaining of the paper ledger. Since its emergence Blockchain technology has been used for various purposes. Different Blockchain consensus and mechanisms have been used to fulfill these purposes. Thus operational Blockchain architectures have been found to date could be classified into three categories.

Public/Open Blockchain: Public Blockchain architecture allows anyone to join the network. Once joined, a user can read, write, and add blocks to the chain. Here, each user's computer is considered as nodes. Each node receives a copy of the Blockchain whenever a new transaction is being committed. A distinctive characteristic of Blockchain, transparency of information is maintained through this type of architecture. In public Blockchain users, personal information is protected. A user's digital signature is used to perform transactions. Hence, the anonymity of the user's identity is preserved [3]. Validation of transactions is done by participating computers in the network. The lucky one gets to solve a mathematical puzzle to register the transaction in a block. For validation labor, users get a reward in cryptocurrencies. This validation process is often termed as mining [1]. An open Blockchain also requires a substantial amount of computational power that is necessary to maintain a distributed ledger on a large scale [4].

Implementation: Bitcoin is built upon public Blockchain technology [5]. Bitcoin is a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going to a financial institution [1]. The Bitcoin network is regulated through Proof of work consensus. By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network and provides a way to initially distribute coins into circulation since there is no central authority to issue them [1].

Earning bitcoin is analogous to mining gold. Hence, computers are in a race to solve a complex mathematical puzzle. Similar cryptocurrencies included Ethereum, Litecoin, Dogecoin, etc

Permissioned/Private Blockchain: Permissioned Blockchain is not accessible to everyone. These Blockchain architecture designed for a specific purpose for a specific group of people. Naturally, they select a subset of the group to validate the transaction. These groups also responsible for designing consensus, on what basis other computers can join/read/write in the network. The regulatory body's existence does not ensure transparency of transactional information to every node. Though centralized in characteristic, valuable information is contained within a handful of peers. Thus security level is enhanced, costs cut down and features greater throughput [4]. In a private Blockchain, because of its operational nature, user identity is not preserved. The organization has rules to know your customer makes user personal information visible to other stakeholders.

Federated/Consorted Blockchain: Federated or Consortium model of Blockchain is another variant of permissioned Blockchain. This type of Blockchain is a private network that operates under the leadership of a group. Those users can read/write transaction details that are pre-validated by network administrators. [4]

Implementation: Hyperledger is built upon private Blockchain technology principles. It's a collaborative effort to facilitate business among cross-industry partners. Every participating agent has a known identity. Participants categorized as Endorser, Committer, and Consenter [2]. A transaction happens when an endorser peer receives a proposal, a batch of block transactions are sent to the committer peers, which then proceed to validate the endorsement policies. Finally, once both of these checks are completed and verified, the transactions are committed to the network's ledger [2]. Additional implantation of permissioned Blockchain is Hashgraph, Corda, etc.

Hybrid Blockchain: As the name suggests, Hybrid Blockchain networks are consist of both public and private Blockchain properties. Participants of such networks can enjoy the privacy of private networks as well as the openness of the public network. In a Hybrid network, Blockchain remains public to its users, whereas access to Blockchain is restricted [6]. An authority empowers with the responsibility to decide who can have access to this network. For example, a school has a restriction to enter its premises for anyone. But students recognized by school authorities are free to roam and can access all of its services. Every entry is required to be recognized by validators. Hence, the user is not anonymous anymore. Moreover, validators can decide what to do with the user's transactional information, as in who is to read/write and audit in the network. Security is preserved for users, as data are available to limited nodes.

Hybrid Blockchain also means an inter-network of Blockchain. For example, in the case of transactions between peers belonged to a different Blockchain network. These networks could as diverse as public, private, and hybrid [7].

Implementation: Hybrid Blockchain networks could be beneficial to cross country businesses and settlements. Blockchain's characteristic to do a fast and secure transaction is appealing in this sector. Generally, this type of settlement requires enormous quantities of paperwork and times delays for different time zones. Countries in different time zones require considerable days to finish businesses and settlements. Blockchain's feature to perform fast transactions and the requirement of zero paperwork could close deals within minutes. Otherwise, that could take several days to weeks. Walt Disney's developed Dragonchain is a hybrid Blockchain platform.

Blockchain's Block Creation:

Blockchains are digital ledgers. It can store millions of transactional information at once. Besides its smooth operation Blockchain also offers security in terms of keeping records. Records once registered in blocks cannot be edited or deleted but can be viewed by everyone. As its name suggests, Blockchain is formed with a series of blocks connected together. Blocks are the basic building blocks of Blockchain technology.

When a transaction is about to happen, details of that transaction need to be verified. For this reason, connected computers in the network compete with each other to validate the transaction. Their competition is fueled by incentive, which is a reward in cryptocurrencies that will be given to that particular computer which will able to validate the ongoing transaction. Generally millions of computers of different computing power participate in this competition. What regulates this race is that a complex mathematical problem needs to be solved first. This problem is generated by the hash function. The computer succeeds to solve the puzzle, is called hashed a block. That implies, upon succeeding to solve the mathematical problem, a hash code is generated by the hash function. This new hash code is assigned to a new block, along with previous blocks hash code stores in the newly formed block, hence, comes the term "chain". The new block contains finished transaction details. These details don't include the purchaser's or seller's personal information. Transactions are registered with a digital signature, some kind of code or username directly associated with the real user. Though transaction details are displayed for everyone to witness, including a digital signature. It is unlikely to reverse engineer that digital signature to its original form. This way user remains anonymous in a Blockchain network.

Once a block is added to the chain automatically connected computers receive a copy of the updated Blockchain. This process goes on 24x7. It is to be noted that the manipulation of transaction details is very unlikely. The first hindrance to doing that, a mathematical problem, upon which, adding a block depends. Second is the hash code assigned to each block and previous blocks. To successfully manipulate blocks hackers need to alter every other block. Blockchain comprises of millions of such blocks. So, this kind of activity wouldn't go unnoticed. Moreover, to get control over the Blockchain network, hacker or group of hackers must have more than half of the total computational power the network operates on. This is because Blockchain has a mechanism to discard any block if found suspicious or altered. The network counts the long chain of blocks. So, it makes sense to alter the Blockchain network one must manipulate its 51% of blocks, hence, more than of computational power consumed by the network. Manipulation is also unlikely because it's economically detrimental to hackers. If they have been able to gain control over 51% of blocks. End users would lose faith and sell their possession or leave the system.

In reality, there's much more scope to be rewarded by staying honest. Bitcoin has a mining threshold. Exceeding the pre-determined threshold result in losing money as a penalty.

Blockchain and Consensus Mechanism:

Proof of Work (POW):

Proof of work consensus is used in bitcoin mining. To sustain a Blockchain network transactions must occur. To validate those transactions connected computers rush in a race. Proof of work is the requirement for a computer to validate a transaction. In other words, the bitcoin Blockchain network runs upon work-based consensus. Computers have to solve an expensive computational problem to verify a transaction. That computational problem is called proof of work. Every node in the network agrees upon these terms and conditions, that's why named as consensus. POW is a work-based approach to reward miners. Blockchains methodology differs in the consensus approach. Proof of work-based Blockchain gives more importance to candidate computer's work or performance. Proof of work is very difficult to solve and easy to verify. As computers do this labor, they need to accumulate enormous computational power. This costs user money in buying hardware and electricity. To inspire miners Blockchain network pays in cryptocurrencies as incentives.

Proof of Stake (POS):

Proof of stake is another consensus mechanism adopted by Blockchain users. In proof of stake approach, to verify a transaction, the Blockchain network chooses a node to hash a block. This choice is based on how much stake one node has compared to the total wealth of the network. For example, if a node has 0.5% of the total network wealth. Then that node can add blocks or verify transactions and earn money worth 0.5 percent of the new blocks. This way network encourages investment. In proof of work approach, work done by nodes gets priority, whereas, in proof of stake, the held value of cryptocurrency gets priority. This priority decides who gets to hash a new block.

Proof of stake algorithm was developed to mitigate the disadvantages of proof of work algorithm. The proof of the work approach needs every node's participation in the network. Only one can be successful. It cost the network in time and energy at the user's end. In POS approach its networks job to allocate the responsibility which is considered much better than the POW algorithm.

Delegated Proof of Stake (DPOS):

Delegated proof of stakes is a variant approach of POS. In this approach, Blockchain network maintenance is done much like an elected government system in a democratic country. In DPOS network users elect a group of people as moderators to look after the Blockchain network. Their job also includes verifying transactions between different users. These advisors get paid for their assigned job. Advisors are selected deciding upon their reputation on the network and acquired the trust of others. Almost 100 users are elected for this job. In this system, the user can evaluate the advisor's performance. In case, chosen bodies aren't doing enough for the wellness of the network. They are subject to thrown out of position [2].

This is the most interactive approach of the Blockchain consensus mechanism. This works best for an active user community. Users are active and well informed about the advisory board. Which makes it possible to regulate them by ordinary users and users regulated by advisory members.

Proof of Elapsed Time (POET):

Proof of elapsed time is entirely a different mechanism. It operates on a time basis. Each user of the Blockchain network has to subscribe under secure software running environments. Under these situations, users have to wait for a certain time to be eligible to hash a new block to the network [2]. This period is allocated randomly among the users. Users waiting for the shortest time get to add a new block or verify the transaction. This a fair policy as the process of allocating the waiting time is genuinely random. POET

consensus is developed by Intel Inc. A software called Software Guard Extension (SGX) runs a trusted program. This program determines whether the user waits for the time they are supposed to. This fair policy of randomly distributing the waiting time ensures fair treatment for every user in the network [2].

Proof of Importance (POI):

Proof of importance is another mechanism for maintaining Blockchain network activities. In this approach, a node with greater importance is selected by the network. Quantification of importance depends on various factors. Here, importance also refers to mining efficiency [2].

After being chosen by the network, the node begins harvesting which is similar to mining in the POS Blockchain system. The selected node can avail hashed blocks transaction fees as a reward.

Unlike the POS approach, In POI system node importance is determined from its overall contribution to the Blockchain network. The determination of an eligible node depends on rating within the system network calculated by the game theory algorithm [2].

New Economic Movement (NEM) cryptocurrency is run by the POI consensus mechanism. NEM cryptocurrency uses three factors to determine eligibility for the allocation of a new block. [2]

- Vesting – process of acquiring threshold vested coins.
- Transaction partners.
- Number and size of transactions of the past 30 days.

Block Structure:

In a Blockchain, every block contains details of the transaction along with a unique hash code for identification.

Main Data: Each block body includes transaction data. These data vary with the purpose of the Blockchain. Usage of Blockchain ranging from the financial sector to supply chain operation. Operational related data are stored in this section of the body.

Timestamps: Timestamps are included date and time of transaction. Each block contains thousands of transaction information. Corresponding data and time are registered with the main data.

Identifier Hash: Each block has a unique hash code. It is generated during Proof of work. When node validates a transaction it’s become eligible to hash a block to the current network. Hash code is generated from the Merkle tree algorithm.

Pointer Hash: Each block in the Blockchain contains a pointer hash, which is the exact copy of the identifier hash of the previous block. Thus a chain of blocks is formed.

Hash Function: Each function has a hash function to generate messages. Hash function processes input into an unpredictable output. Through these messages, nodes communicate among themselves. Blocks also change their state upon receiving messages [3].

Blockchain vs Database:

Often it is a matter of confusion whether Blockchain is a database. Can we use those two-term interchangeably? The answer is no. Database and Blockchain are two different approaches to store information. In the database, records are saved first, validated, and audited later. Where in the Blockchain each transaction validated at the time of entry. The database allows a record to be edited/deleted/updated from the archived database. Blockchain does not allow records to be modified. Once records are registered, they will be there for eternity, if not discarded for saving disk space. The database is generally administered by one entity or several delegates allowed to administer the database. Blockchain is regulated by its computers on the network. These two have differences in their applicability too. In simple terms, databases are centralized, permissioned, and requires administration, whereas Blockchain is decentralized, public and no administration requires [8].

Blockchain Wallet:

This refers to a digital wallet. The owner of the wallet has two keys, public key, and private key. A public key is used to deposit or withdraw cryptocurrency from the wallet. The private key is for accessing the wallet. The public key is a shorthand version of the private key. A new public key needs to be generated for each transaction. Public keys are called digital signature in the cryptocurrency domain. Blockchain's transparent characteristic makes public keys visible to all users. Since public keys are a digital signature, the user's identity is not disclosed in this case. Blockchain wallet is analogs to the physical mailbox with a lock. Anyone can send something into the mailbox, but only the owner can open it through the appropriate key. If the owner loses the key, he can't open the mailbox. That is also true for the Blockchain wallet. If the owner forgets the private key of his wallet, the wallet cannot be retrieved. This is due to the fact that Blockchain does not store user information.

Advantages of Blockchain:

Decentralization: Blockchain is a decentralized architecture. Due to this fact, there is no need for an intermediary body. Intermediaries help with negotiation or transaction. In exchange for that help, a good amount of money is charged. Blockchain's decentralization character requires no middle man. Blockchain technology has its proof of validation and authorization technique, which is unique to any other system [9]. Due to the lack of top-down hierarchy or central authority, every node gets to participate in the process. That ensures cooperation and coordination among users in the macrosystem [10].

Data Immutability: Blockchain's block and chain structure make inside data impossible to tamper. Each block contains all transaction information along with parent blocks hash code. Data stored in Blockchain are immune to attack compared to database stored data. If any blocks information has been altered by a malicious attack, Blockchain has a protocol to alert all the nodes in such a situation. Node altered is being discarded from the chain of blocks.

Guarantees Data Security: Blockchain has encryption and decryption algorithms. This enables the hash function to generate output which cannot be reversed. Public and private keys are another example of an encryption algorithm. Public keys are shorthand notation of private keys. Though, public keys are visible to all and used for the transaction. It is necessary to note that decipher of public keys is impossible to do.

Data Consistency: In a distributed network, the Byzantine Fault-Tolerant (BFT) problem caused by the participation of millions of nodes at a time [10]. To avoid these problems Blockchain has a consensus mechanism for production and verification of data block. The adoption of this mechanism puts a

safeguard for data inconsistency. The mechanism ensures the sender and receiver's balance information is valid. This way data consistency in a block is preserved.

Transparency: When Blockchain performs a transaction, it is validated through nodes in the network. After successful hashing, a new block is added to the existing block structure. Every node receives a copy of the updated Blockchain. Anyone connected to the network can read/write/audit the information, as Blockchain demands transaction information to be shown publicly. In this way, the transparent characteristic of Blockchain ensures data transparency.

Secure Transaction: Transaction in physical level needs an intermediary as a proof of transaction. Often that is biased or unable to settle a dispute. In such a case three parties' identity is at stake if the deal won't go as planned. But Blockchain offers anonymous transactions that secure a participating agent's identity and eliminates associated risk with the disclosure of identity. Blockchain also eliminates middleman negotiator. Hence, biasedness vanishes with it. In terms of a physical transaction, paper ledger could be damaged intentionally or unintentionally. Blockchain offers a permanent digital record of the transaction. In this respect, the possibility of paper fraudulent becomes zero.

Open Source: Blockchain technologies offer tools for free to anyone to create his application. This application will serve its creator's purpose as well as fertile the field of digital cryptocurrency.

Disadvantages of Blockchain:

51% Attack: Though Blockchain is decentralized and empowered with a high-level encryption algorithm, it has vulnerabilities too. Like other digital platforms, Blockchain could be attacked, though stakes are very low.

Every computer across the network has a copy of the Blockchain. After each transaction Blockchains get updated with a new block at the end of the chain. This process is called hashing. If a group of people manages to accumulate half of the computational power consumed by the entire network and passes proof of work verification. That group will likely have control over the entire chain of blocks. In a bitcoin network 51% attack would follow these steps: publishing mining software at higher EV (expected value), creating a pool with unwanted stickiness, creating unwanted coalitions, attacking other pools with cannibalizing pools, switching to members only [11].

Illegal transaction: Blockchain architecture offers users anonymous participation in the network. Which poses a great threat to society. Taking advantage of this feature illegal purchase of marijuana, drugs, and extortion, even murder contracts are given on the dark web. All kinds of illegal transactions are committed by cryptocurrencies and it is very much impossible to trace the identity. To date, an efficient method has not been found to undermine Blockchain's high-level encryption.

Time Inefficient: Blockchain reportedly needs 10 minutes to perform a transaction [3]. It is because of the consensus algorithm. Obeying a consensus algorithm every node must show proof of work. This will be verified and money will be transferred indicating the end of the transaction. Corresponding details will then be recorded. Its time consuming not only because of proof of work consensus but also for crowded nodes in the network. VISA Inc. is thousands of times faster than Blockchain in terms of the transaction.

Redundancy: In Blockchain architecture designed with proof of work approach, every node races to solve a mathematical problem. Eventually one becomes successful. In terms of energy losses or

redundancy of work done, we can observe that a lot of computational power is required to perform merely one transaction. This redundancy of work done is a considerable fault in Blockchain architecture [12].

Users Privacy: Immutability and transparent characteristic of Blockchain could harm the user's privacy and reputation. Every node receives a copy of the Blockchain after each transaction. This could mean a violation of someone ‘s privacy [13].

Smart Contract: Smart contract is a computer program first proposed by American scientist Nick Szabo [14]. This program is written by users according to their own needs. A smart contract program runs on a public Blockchain network, unlike a traditional programming language that runs on IDE. Users need to define the parameters and purpose of this program.

Cryptocurrencies are built upon Blockchain technology. Smart Contracts are built on top of that cryptocurrency platform. Blockchain offers architecture of network for secure transactions. Among many of Blockahins applications, the smart contract is most recent and a matter of interest among countless scholars and business executives. In simple terms, Smart Contract is termed as a “trusted third-party” between two or more users [15]. Users are generally agreed to do some kind of transaction based on pre-defined rules. These rules create a scenario when conditions will be met, a transaction will occur. This could think of as a one-way transaction. Once a smart contract is created, no matter what happens, it will be executed. In terms of creating a smart contract for two individual users, all the users across the network must endorse smart contracts terms and conditions. It also works as a witness for a transaction.

Smart Contract Creation:

Blockchain eliminates intermediary bodies in a transaction process. As a result transaction cost reduces to a great extent and security is ensured. This is true for the present time’s transaction. Transactions may occur between two or more users based on the fulfillment of some conditions. Transactions that are scheduled to occur in future time are not included in the scope of Blockchain's primary objective. To address this need, a new concept has been introduced, which is a Smart Contract. The type of transactions that ought to occur with some conditions needs an intermediary middle man. This intermediary body will ensure the transfer of funds. In our daily life, physical intermediary institutions or personnel charge an amount exchange for this task. But the idea of Smart Contract is a digital intermediator. This intermediator resides in public Blockchain. Now why digital intermediator is free of cost to use, whereas physical intermediator charges a lot. The answer to this question comes from Blockchain’s characteristic of being decentralized. Decentralized means, there is no central authority to decide on the network's operation. Rather network operation is performed upon pre-determined consensus algorithm. There is no central authority to act as an intermediator. So, to perform a conditional transaction, there is a universal agreement among all users across the network that is to build their digital intermediator. This is a smart contract. A smart contract is a statement of the agreement upon which pre-defined promised transactions will be executed.

Smart Contract Structure:

A smart contract is a user-defined computer program code. Upon meeting the deadlines, these program codes are executed by the connected nodes of the Blockchain network. A smart contract is consist of three parts:

- Program Code

- Storage File
- Account Balance [15]

For programming purposes of smart contracts, there have been many high-level languages for different platforms of cryptocurrency. One such is Solidity and Python Programming Language used for smart contract creation in the Ethereum platform [16]. The code written for a smart contract is not editable or cannot be deleted at any circumstances once created. Posting a transaction in the Blockchain network is required, whenever the user intends to create a smart contract.

Smart Contract Execution:

For the execution of a smart contract, participants of the network need to act accordingly. After execution Blockchain updates itself and miners receive a copy of the Blockchain. Multiple contracts can be created. Execution of one contract may depend on another smart contract. In the case of an independent smart contract, it is executed when invoked by a user. Participants of the transaction agreed upon the outcome of the smart contract execution sends a message to the program code for invoking it. Upon invoked, program code executes and a transaction occurs. That's way smart contract programs have an instruction in their code, which works as a message sender or receiver. For multiple smart contracts involved in a single transaction scope, different smart contracts have to send messages to each other in proper order. Whenever a smart contract receives a message, it executes to transfer the currency to the winner's wallet. Hence, a smart contract program contains the sender and receiver both party's public key in its code. During execution, smart contracts can read from and write in the data storage file. Its structure enables it also to receive and send money.

Advantages of Smart Contract:

Smart contract has the potential to revolutionize the business sector. It could be a digital asset or a physical one, the smart contract ensures cheap and risk-free processing of both, efficiently from supplier to buyer. Some application advantages of a smart contract are given below.

Risk Reduction: In the context of doing transactions via smart contracts, the risk of losing money is completely gone. Smart contracts program will be executed no matter what happens, which invariably means the transfer conformation of pre-deposited money. In this way, transaction risk in the contractual agreement is done effortlessly.

Cost Reduction: In absence of a physical intermediary cost of the transaction comes down. Blockchain's decentralized architecture offers settlement of contractual agreement through a user-defined program. As written in its instruction set, a smart contract will run as soon as conditions are satisfied. It requires no cost to write code. Above all, as the Blockchain network is open for anyone, so is the smart contact facility. Thus, it requires skills to create smart contracts.

Business Efficiency: Smart contract smooth business operation over Blockchain technology. In an example of a supplier and buyer, the supplier gives a product catalog, the buyer commits order, the buyer receives the product and sends a message to the smart card. Upon satisfying this condition, smart contract transfers money from buyer to supplier. Smart contact has access to supplier and buyer wallets public keys for deposit and withdraws operation [17].

Fast Settlement of Agreement: In a smart contract, agreement terms are explicitly mentioned in the program code. It could appear as a nightmare while performing transactions requires multiple party's involvements. Compared to settlement performed by physical intermediator, smart contracts are swift and efficient. Whereas conventional ways may take hours to days, smart contract performs even complex contractual agreements in a fraction of a second.

Backup: Physical contract documents can be damaged or manipulated. But in a smart contract, the digital agreement cannot tamper. Transaction records reside in the Blockchain. So, they are always traceable.

Disadvantages of Smart Contract:

Buggy Code: Smart contract agreements are written in a programming language like Solidity, Go, Kotlin, Java [17]. So, it is expected that long and complex smart contract programs will be more or less buggy. It takes a lot of effort to fix bugs in code, otherwise, it may lead to an unexpected outcome.

Readability: Smart contracts are computer programs but nothing. So it is difficult for people to read and understand agreements written with conditional statements. It has been proposed to implement a semi-automated translation system to convert human-readable contractual agreements into computational programs [18]. We can expect, this would mitigate the issue.

Programming Cost: Without programming transaction in a smart contract is not possible. Moreover, this task needs a skillful programmer. No one would risk his money. So, the implementation of a transaction has cost to some extent provided that the participating agent unable to do programming the job himself.

The rigidity of agreement policies: In a real-world scenario, agreement policies could be changed if needed. It is expected that in the long term agreement, the situation will not be the same as is now. In a smart contract program, these agreement terms and conditions are fixed. They cannot be amended if necessary. This rigidity makes a smart contract a less viable option for everyday use [19].

Privacy: Blockchain technology is a distributed ledger. All information resides in Blockchain are visible to all nodes. Nodes remain anonymous while doing transactions. But privacy is lost, when it comes to transaction details. One user may not want to disclose the details of his agreement with other nodes in the network. But this is not possible in a smart contract. Buterin argues that focus should be given in this privacy area because the existence of transactional ledger in public domain lapse privacy, provided users are anonymous [20].

Conclusions: Smart contract is embedded in Blockchain technology. It is a clever way of utilizing Blockchain's powerful architecture and consensus algorithm. Smart contracts innovative idea is based upon Blockchain's unique combinations of features. Blockchain's decentralization feature makes it possible for smart contract to be cost-free and reliable, though the absence of authority creates scope for illegal activities. The distributed feature helps to build Blockchain users a community where they can trust to conduct the business of physical products along with digital ones. Smart contract facilitates the online contractual transaction, it doesn't guarantee an honest deal. In terms of Blockchain, transparency is a doubtless extra-ordinary characteristic. For smart contract applications, it is not so. Participants of a smart contract transaction may feel uncomfortable sharing their transaction details. Nonetheless, Blockchain and its embedded technology smart contract have tremendous potential to disrupt the conventional way of doing business.

References:

[1] S. Nakamoto, "A peer-to-peer electronic cash system ", 2008. Accessed on: July 2, 2020. [Online]. Available URL: https://bitcoin.org/bitcoin.pdf

[2] A. Welfare, "Commercializing blockchain (strategic applications in the real world) || types of blockchain", 2019. Accessed on: July 2, 2020. [Online]. Available doi: 10.1002/9781119578048.ch2

[3] AKM. B. Haque and M. Rahman, "Blockchain technology: methodology, application and security issues", *IJCSNS*, vol. 20, no. 2, 2020.

[4] Morkunas, V. J, J. Paschen, and E. Boon, "How blockchain technologies impact your business model", *Business Horizons*, vol. 62, no. 3, pp. 295-306, 2019

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? - a systematic review", *PloS One*, vol. 11, no. 10, pp. e0163477, October. 2016, Accessed on: July 2, 2020. [Online]. Available doi: https://doi.org/10.1371/journal.pone.0163477

[6] M. Wazid, A. K. Das, S. Shetty and M. Jo, "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things," in *IEEE Access*, vol. 8, pp. 88700-88716, 2020, doi: 10.1109/ACCESS.2020.2992467.

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

[8] V. Tabora, "Database and blockchains, the difference is in their purpose and design", *Hetnet*, vol. 13, 2018

[9] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Vilnius, 2018, pp. 1-6, doi: 10.1109/AIEEE.2018.8592253.

[10] L. Wen, L Zhang, and J.Li, "Application of blockchain technology in data management: advantages and solutions", *In: Li J., Meng X., Zhang Y., Cui W., Du Z. (eds) Big Scientific Data Management. BigSDM 2018. Lecture Notes in Computer Science*, 11473, Accessed on. 3 July, 2020. [Online]. Available doi: https://doi.org/10.1007/978-3-030-28061-1_24

[11] J. H. Park, and J. H. Park, " Blockchain security in cloud computing: Use cases, challenges, and solutions", *Symmetry*, vol. 9, no. 8, p. 164, August. 2017, Accessed on: 3 July, 2020, [Online], Available doi: https://doi.org/10.3390/sym9080164

[12] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of blockchain technology: pros cons and SWOT", *Cluster Comput 22*, pp. 14743–14757, 2019, Accessed on: 3 July 2020, [Online], Available doi: https://doi.org/10.1007/s10586-018-2387-5

[13] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaría, "To Blockchain or Not to Blockchain: That Is the Question," in IT Professional, vol. 20, no. 2, pp. 62-74, Mar./Apr. 2018, doi: 10.1109/MITP.2018.021921652.

[14] M. Giancaspro, "Is a 'smart contract' really a samrt idea? Insights from a legal perspective", *Computer law & security review*, vol.33, no.6, pp. 825-835, December. 2017, Available doi: https://doi.org/10.1016/j.clsr.2017.05.007

[15] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, " *Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab", In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science*, vol. 9604, 2016, Available doi: https://doi.org/10.1007/978-3-662-53357-4_6

[16] I. Karamitsos, M. Papadaki, and N.B. Al Barghuthi, " Design of the Blockchain Smart Contract: A Use Case for Real Estate", *Journal of Information Security*, vol. 9, pp. 177-190, Available doi: https://doi.org/10.4236/jis.2018.93013

[17] Z. Zheng, S. Xie, H. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, " An overview on smart contracts: Challenges, advances and platforms", *Future Generation Computer Systems*, vol. 105, pp. 475-491, April. 2020, Availavle doi: https://doi.org/10.1016/j.future.2019.12.019

[18] C. K. Frantz and M. Nowostawski, "From Institutions to Code: Towards Automated Generation of Smart Contracts," 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), Augsburg, 2016, pp. 210-215, doi: 10.1109/FAS-W.2016.53.

[19] S. Nzuba, "Smart Contracts Implementation, Applications, Benefits, and Limitations ", *Journal of Information Engineering and Applications*, vol. 9, no. 5, September. 2019, Available doi: 10.7176/JIEA/9-5-07

[20] V. Buterin, "A next-generation smart contract and decentralized application platform", *white paper*, vol. 3, no. 37, January. 2014, Accessed on: 3 July, 2020, [Online], Available URL: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf