iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42905

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Ethereum Blockchain Wallets

Himank Goel[1], Harshit Gupta[2], M.L. Sharma[3], K.C. Tripathi[4]
[1, 2, 3, 4]*Maharaja Agrasen Institute of Technology, Delhi*

Abstract: Blockchain technology is an evolving technology which is revolutionizing the IT industry by providing better security and efficiency. This technology can help to solve different kinds of problems in the industrial sphere, such as trust, transparency, security and reliability of data processing. I theory, the use of Blockchain technology shows great and positive results. Ethereum is the most widely used blockchain platform because of its unlimited block size. Many sophisticated problems with smart contracts can be solved with Ethereum and the removal of any third party organization which may interfere in transactions and it is easier to implement compared to other blockchain technologies. In this paper the benefits and drawbacks of wallet based on Ethereum blockchain are analyzed. Many already implemented wallets on Blockchain technology were studied, as well as affected success or problems factors during the implementations. This paper aims to analyze conveniences and difficulties related to the Blockchain integration to a wallet and implementation in the different fields of modern industry.

I. INTRODUCTION

Blockchain technology was first introduced by Satoshi Nakamoto in November, 2008. The idea was to make transactions electronically without any central authority at a low transaction fee [1]. Initially, blockchain was used to exchange bitcoins over the network. Due to its usability, it has expanded and is now also being used in several other applications such as smart cities, retail, healthcare, smart transportation and authenticating IoT (Internet of Things) devices [2][3]. IoT devices are widely adopted for automation[4][5] and blockchain can prevent unauthorized access to such devices. It can help to make the business, government and logistic systems more reliable, trusty and safe. Certainly, the Blockchain technology has some disadvantages, such as the costs, environmental problems and the implementation process of the technology.

Ethereum is a blockchain platform. It is a technology that's home to digital money, global payments, and applications. The community has built a booming digital economy, bold new ways for creators to earn online, and so much more. It's open to everyone, wherever you are in the world – all you need is the internet.[6]

At the heart of the Ethereum platform are smart contracts. A smart contract is simply a non-modifiable general purpose computer program. Ethereum not only hosts smart contracts, but can also execute them. Smart contracts can be written in Solidity, Vyper, Yul, DAML but mainly in Solidity. Smart contracts are commonly used to create a tradeable digital token, which can represent a currency, an asset, a virtual share, a proof of membership, etc[7]. Smart contracts can also be used for creating immutable contracts such as a shared wallet with wide applications such as giving allowances to employees, budget allocation to contractors in businesses.

II. BACKGROUND: BLOCKCHAIN, ETHEREUM AND SMART CONTRACTS

A. Blockchain

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value" – this statement is one of the most popular definitions of the Blockchain, which was developed by Don and Alex Tapscott [8].

More specifically, transactions are packaged into blocks and these blocks are linked to one another as a chain. Once a block is appended to a blockchain, its contents cannot be altered without changing every other block that came after it. In practice, a transaction in Ethereum is deemed final and irreversible after six block confirmations. More generally.

B. The structure of the Blockchain Technology

A blockchain is a growing list of records, called *blocks*, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.[9].

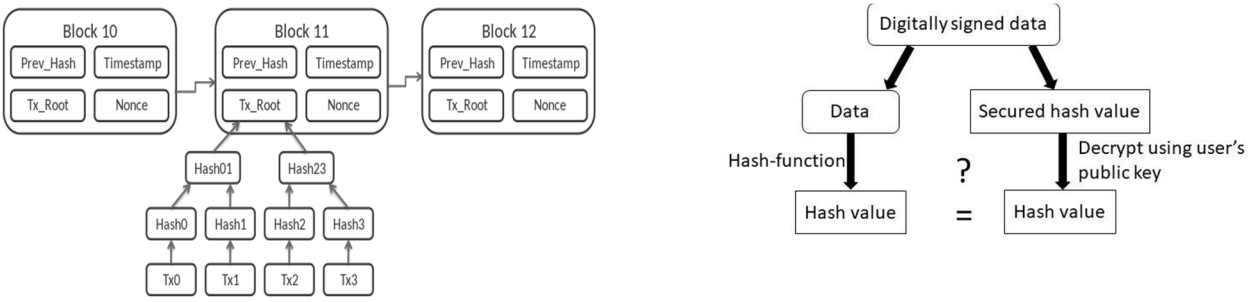
Each block contains the cryptographic hash of the previous block.

All hash's information is generated automatically, it means that it is not possible to change any information in the hash. In this case, each next block amplifies the verification of the previous block and the security of all Blockchain. The more blocks in the chain - the safer and more reliable the Blockchain [32].

In fig 1, every block contains the hash of the previous block, time at which block was appended to the blockchain network. As it follows the Structure of a Merkle Tree, every node also stores the state root, i.e, the root hash of a specialized kind of Merkle tree which stores the entire state of the system: all account balances, contract storage, contract code and account nonces are inside.

This would involve two steps, generating hash of the message and signature decryption. By using the signer's public key, the hash could be decrypted. If this decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer.

(Fig. 1)



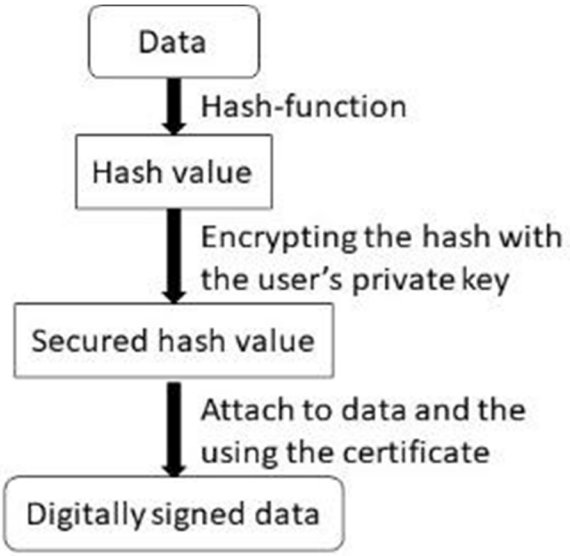


Fig. 2. The signing process in the Blockchain

Fig. 2 shows the signing process, which includes the signing with the private key and certificate.

Digital signatures are nearly impossible to forge due to their use of number theory to guarantee functionality and use a system called public key cryptography in which users own both a public key and a private key, forming a pair. The public key (Fig. 3). This would involve two steps, generate a hash of the message and can be thought of as the identity of the owner and the private key can be thought of as secret information that allows the owner to prove their ownership of the public key.

The process of the block creation is shown in Fig. 4. In this case, each block included the previous hash value, the timestamp, the merkle root and nonce.

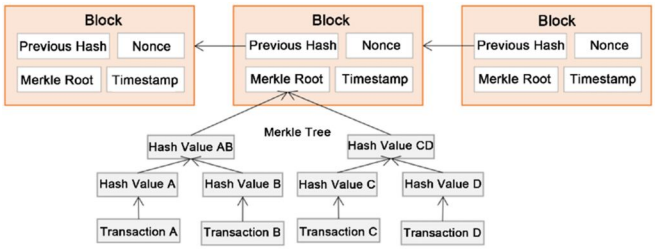


Fig. 4. The structure of the Blockchain [8]

C. Proof of Work (PoW)

Proof of work (PoW) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system.

Introduced in 2009, Bitcoin became the first widely adopted application of PoW idea. The Proof of Work is the algorithm of security. The mining is the process of solving a computational challenge imposed by the PoW protocol. The node, which wants to participate in mining, uses the PoW protocol for the affixation of the block to the Blockchain. In this case, the node must choose the block with the biggest hash's value and after that it can attack the block, [10].

D. Smart Contracts

A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement. The objectives of smart contracts are the reduction of need in trusted intermediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions. Similar to a transfer of value on a blockchain, deployment of a smart contract on a blockchain occurs by sending a transaction from a wallet for the blockchain. The transaction includes the compiled code for the smart contract as well as a special receiver address. That transaction must then be included in a block that is added to the blockchain, at which point the smart contract's code will execute to establish the initial state of the smart contract. Byzantine fault-tolerant algorithms secure the smart contract in a decentralized way from attempts to tamper with it. Once a smart contract is deployed, it cannot be changed. Smart contracts on a blockchain can store arbitrary state and execute arbitrary computations. End clients interact with a smart contract through transactions. Such transactions with a smart contract can invoke other smart contracts. These transactions might result in changing the state and sending coins from one smart contract to another or from one account to another[11].

On the Ethereum blockchain, smart contracts are essentially Ethereum accounts. They might have a balance and the user can interact directly with them to carry out transactions over the network. But they are deployed on the Ethereum blockchain and run as programmed. User accounts can then transact with a smart contract deployed on the network by submitting transactions which will in-turn execute a function defined on the smart contract.

Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible.

E. Ethereum

Ethereum is a flexible Blockchain platform which is open to use by everyone. This platform has a high level of security from different kinds of attacks. The users can create the Smart contracts and decentralized applications.

Ethereum is an online, blockchain-based exchange protocol created by Vitalik Buterin in 2015. The Ethereum network is made up of thousands of computers connected to each other through the Internet. Ethereum allows users to mine the cryptocurrency named Ether by creating smart contracts that verify every transaction and are recorded in a public blockchain. The remuneration in cryptocurrency compensates for the material and energy costs linked to the provision of this computing power. The ethereum network also allows developers to build and deploy decentralized applications (DApps). These DApps are also stored on the blockchain.

DApps are 'open-source' software that uses blockchain technology. Unlike traditional applications, they do not require an intermediary to operate. Two important characteristics that all DApps have in common are the fact that they are open-source (autonomously governed) and decentralized. Smart contracts are used to create the DApps. Smart contracts are formed using the 'Ethereum Virtual Machine' (EVM). Once a smart contract is running on the blockchain, it acts as a computer program that operates on its own. They operate as scheduled, without censorship, downtime, or third-party influence.

"Ethereum, taken as a whole, can be viewed as a transaction-based state machine."

In the Ethereum network, in order to create a smart contract, a contract account needs to be deployed. Unlike the externally owned account, creating a contract account has a cost since it is using the network's storage. Another key difference between the two accounts is that a contract account can only send transactions in response to receiving a transaction. Furthermore, transactions from an external account to a contract account can trigger the smart contract code which can execute many different actions, such as transferring tokens or even creating a new contract.

An Ethereum account, be it an externally owned account or a contract account has four fields that make up its state

1) *Nonce:* A scalar value equal to the number of transactions sent from an externally owned account address or, in the case of a contract account, the number of contract-creations made by this account. This number ensures transactions are only processed once.
2) *Balance:* A scalar value equal to the number of Wei owned by the account. Wei is the smallest sub denomination of Ether, where one Ether is equal to 10^{18} Wei.
3) *Code Hash:* For externally owned accounts, this field is populated with the hash of an empty string. For contract accounts, this is the code that gets executed when the account is triggered, this field is immutable, as such it cannot change once it is constructed
4) *Storage Root:* A 256-bit hash of the root node of a Merkle Patricia trie that encodes the storage contents of the account

F. Solidity

Solidity is an object-oriented, high-level language for implementing smart contracts on the Ethereum blockchain. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state. Solidity is a curly-bracket language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features. With Solidity, contracts for use cases such as voting, crowdfunding, blind auctions, and multi-signature wallets. For Solidity, a dedicated IDE(Integrated Development Environment) known as Remix is used. On Remix, Smart contracts can be implemented and deployed at the same time. The structure of a Solidity smart contract resembles that of a class (as in object-oriented programming).Similarly to the Java compiler, the Solidity compiler also produces a bytecode version of the source code, which is executed by the Ethereum Virtual Machine (EVM). The Ethereum bytecode is an assembly language made up of several opcodes (low level instructions).

G. Wallets on Blockchain

Wallets keep valuables, credentials, and items for access rights (like cash, licenses, credit cards, key cards) in one place, for ease of access and use. On the blockchain, cryptocurrencies play a role similar to cash, while cryptographic tokens are a universal tool for handling rights and assets. Blockchain wallets manage the cryptographic keys required for authorization and implement the protocols for interacting with blockchains.

Smart contracts are one of a kind disruptive financial technology, and crypto tokens are often termed the excellent application of smart contracts. They already started to change financial processes and markets.

Wallet contracts hold cryptocurrencies and access to tokens and may offer advanced methods for manipulating the assets. Simply by introducing the role of an 'owner' it becomes possible to transfer all assets of a wallet contract transparently and securely in a single transaction. More refined methods include multi-signature wallets, which grant access only if sufficiently many owners agree.For the management of cryptocurrencies or cryptographic tokens, many users employ a software wallet that facilitates the interaction with a blockchain in general or with on-chain programs (smart contracts) in particular. While many blockchain wallets execute their core program code off-chain, some wallets implement core functionality on-chain as smart contracts with the intent to increase trust and security by using transparent and verifiable execution[12].

Types of Wallets

Based on their features, wallets can be divided into six wide groups:

1) Simple Wallets: provide little extra functionality beyond handling Ether and tokens.
2) MultiSig Wallets: require that m out of n owners sign a transaction before it is executed. Usually the required number of signatures (m) is smaller than the total number of owners (n), meaning that not all owners have to sign. In most cases, the set of owners and the number of required signatures can be updated.
3) Forwarder Wallets: forward the assets they receive to some main wallet.

4) Controlled Wallets: can be compared to traditional bank accounts. They are assigned to customers, who can use them as targets of transfers, but the control over the account remains with the bank.
5) Update Wallets: provide a mechanism to update their main features at the discretion of the owner.
6) Smart Wallets: offer enhanced features like authorization mechanisms for arbitrary transactions, recovery mechanisms for lost keys, modular extension of features, or advanced token standards.

III. THE BLOCKCHAIN ADVANTAGES AND DISADVANTAGES

A. *The advantages of the Blockchain*

Blockchain technology is a decentralized system and it is the main benefit of this technology. Why is it important for our life? The answer to this question is very simple – it is not necessary to work with a third-party organization or with the central administrator.

It means that the system works without intermediaries and all participants of this Blockchain make the decisions.

Each system has the database and it is important to protect this database, because when the system is working with the third-party organizations, there is a hacking risk of the database or the data may turn up in the wrong hands. The process of database security might take a lot of time and might cost a lot of money. If we use Blockchain technology this can be avoided, because the transactions of the Blockchain have their own proof of validity and authorization to enforce the constraints. And it means that the transactions can be verified and processed independently [8], [14]

Each action is recorded to the Blockchain and the data of records are available to every participant of this Blockchain and cannot be changed or deleted. The results of this recording give the Blockchain's transparency, immutability and trust [8], [15].

The trust of the Blockchain is based on the belief of two or more participants, who do not know each other. The main idea is the real and not worthless transactions between these unknown people. The trust can be increased further, because there can be more shared processes and records [16], [14].

The immutable is achieved when the transactions are agreed and shared across the Blockchain. When the transaction is connected to the Blockchain, it won't be possible to change or delete it. It also depends on the system's kind – if the system is centralized, it can be changed or deleted, because the decision is made by one person. But if the system is decentralized, such as the Blockchain, there each transaction, which is joined to the Blockchain, is copied to each computer in this Blockchain network. This benefit makes the Blockchain technology unalterable and indestructible. The users of the Blockchain have the power to control all transactions and information.

To change or delete the information into the Blockchain is possible when an intruder has the fantastic computing power to be able to overwrite or delete the information on all computers, which includes into the Blockchain before the next block recorded here. If the Blockchain consists of a small number of computers, the technology is more exposed to be attacked – if there are a lot of computers into the Blockchain then the system becomes safer and more transparent [8], [15], [16], [17], [14].

The transparency of the Blockchain is achieved on the transactions copying process. As it was written above, each transaction is copied to either computer in the Blockchain network. Every participant can look at all transactions, also it means that each action is shown to participants of the Blockchain. Nobody cannot do anything insensibly [16], [17].

The Blockchain designs in a way that it can show any problems and correct them if it is necessary. This advantage makes the Blockchain technology traceable [12].

The high security of the Blockchain technology is achieved on the individual entry into the network. Because each person who enters the Blockchain is provided with a unique identity which is linked to his account. Another reason for the Blockchain security is the reliable chain of the cryptographic hash.

When a new block is created, it is necessary to calculate the hash value for the new block. The new hash surely includes the previous hash's value. In general, the hash consists of the type, the block's ID number, the previous hash's value, the time when block was created, the user ID number, the miner's level and the merkle root with the information about previous transactions and its hashes. This hash is generated automatically by the node-key. In this case, it is impossible to change any information in the hash value [12].

The last one advantage is the faster processing. Traditionally, the transaction takes a lot of time in processing and initializing into a banking organization. The use of the Blockchain technology helps to reduce the time for the processing and initialization to many times – from approximately 3 days to several minutes or even seconds [17], [12].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

B. The Blockchain Disadvantages

If the Blockchain has advantages, this technology has disadvantages or challenges.

The main disadvantage of the Blockchain is the high energy consumption. The consumption of power is needed for keeping a real-time ledger. Every time the new node is created and at the same time it communicates with each other node. In this way transparency is created. The network's miners are attempting to solve a lot of solutions per seconds in efforts to validate transactions. They are using substantial amounts of computer power. Every node is giving extreme levels of fault tolerance, ensures zero downtime and is making data stored on the Blockchain forever unchangeable and censorship-resistant. But these actions burn electricity and time – it is wasteful, when each node repeats the achievement of Consensus [8].

The signature verification is the challenge of the Blockchain, because each transaction must be signed with a cryptographic scheme, the big computing power is necessary for the calculation process to the sign. It is one of the reasons for the high energy consumption [8].

The next problem of the Blockchain is the opportunity to split the chain. The nodes, which are operating on the old software, won't accept the transactions in the new chain. This chain is created with the same history as the chain, which is based on the old software. It is named the fork. There are two kinds of forks – the soft fork and the hard fork [13], [14].

The soft fork establishes the new ruleset to the blocks in the protocol. The nodes are updated to enforce the soft fork's rules. If the block, which was considered valid before, does violate the new soft fork rules, the block won't be considered after the soft fork activation.

For example, the soft fork is restricting the block size to 500 kB, but before was the 1 MB. It means that the blocks, which are larger than 500 kB, won't be valid in the new chain after upgrades [13], [14].

The hard fork loses the ruleset to the blocks in the protocol. This process is the same with the soft fork process, but the value and result of it is the opposite. For example, the hard fork is increasing the block size to 2 MB from 1 MB. If the block has gone through all the rules of the hard fork, the block will be accepted, even if the block was not in the chain before [13], [14].

Another problem of the Blockchain is the balance between the nodes' quantity and the favorable costs for users. Now the nodes are lacking for the Blockchain correctly and powerful work. In this case, the costs are higher, because the nodes received higher rewards; but the transactions completed more slowly, because the nodes do not work intensively [14].

The Blockchain has grown when the new blocks affiliate to the chain and the computing requirements increase. Not all nodes can provide the necessary capacity. There are two problems: the first is the smaller ledger, because the nodes can not carry the full copy of the Blockchain and it breaks the immutability and transparency of the Blockchain; the second is the Blockchain becomes a more centralized system [14].

The high costs are a big disadvantage of the Blockchain. The average cost of the transaction is between 75 and 160 dollars and most of it is covered by the energy consumption [12]. One of the reasons for this situation has been described above. The second reason is the high initial capital costs of the Blockchain [8].

C. The Attacks and Problems of the Blockchain

The Blockchain can be attacked by the different threats, which are connected with the PoW and PoS protocols. Most of them are almost impossible [7], [11], [18].

1) *Attack of 51%:* It will happen when two miners are calculating the hash of the block at the same time and get the same results. In this case the Blockchain will split and as the result, users have two different chains, and both are considered true.
2) *Double-Spending:* Principle of this attack is the same as the previous attack, but here can be used to split of the chain to spend the money again.
3) *Sybil's Attack:* It's possible when one node accepts several essences, because the network can't authentically distinguish the physical machines. Sybil's attack can help to fill the Blockchain with users under its control. It can lead to the previous two attacks and the ability to see all transactions with special programs.
4) *DDos's Attack:* The attack consists of a large number of similar requests. There is the protection in the DDos's attack – size of the block up to 1 MB, size of each script up to 10000 bytes, up to 20000 of the signatures can be checked and maximums of the multiple signature is 20 keys.
5) *Cracking Cryptography:* It is possible to use quantum algorithms such as 'Shora' which can break the RSA encryption. The scientists work on the cryptographic algorithms, which are based on the hash functions.

IV. CONCLUSION

The Blockchain is the new type of the database which can solve some of the problems in the centralized system, such as the transactions without a middleman, the spent time on each transaction, protection against the unintentional or modification of data in the Blockchain.

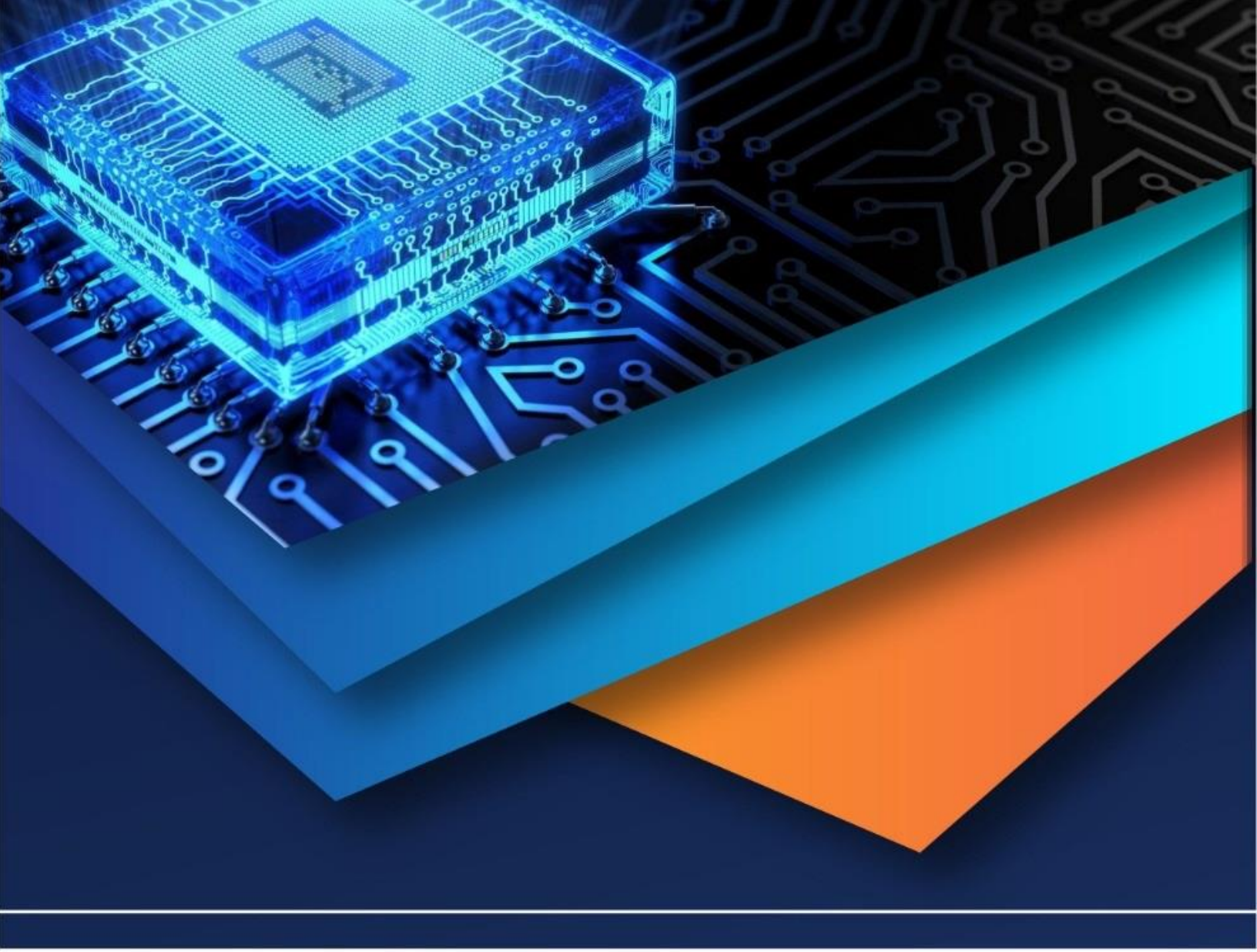
With the advantages of the technology, such as the transparency, anonymity, the multiple copying of the transactions and the decentralized digital ledger, the Blockchain technology is reliable and not destructible, and attacks could disrupt the system work, not the technology. There are only a few examples of Blockchain actually getting hacked in practice.

Blockchain technology is useful and versatile for our world and is also a futuristic technology, because it can accommodate a wide number of applications single handedly, but it is pretty new and its implementation is little studied in practice. Blockchain technology promises us a bright future without fraud and deception. The developers must devote more time to the practical application and implementation of the Blockchain into the already existing systems of the main industrial directions such as financial transactions, IOT, supply-chain demand because the Blockchain can bring honest and trusty business, government and logistic systems. The challenges of the Blockchain are arduous, but the results of the Blockchain being used in so many fields outweighs by a far greater margin.

It is necessary to keep exploring the Blockchain development and application in the different areas for the nearest future, because this new technology can help to solve many difficult problems, which are disturbing and preventing correctly systems work.

REFERENCES

[1] H. Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, "Blockchain for the IoT and industrial IoT: A review," Internet of Things, vol. 10, p. 100081, 2020.
[2] S. K. Singh, S. Rathore, and J. H. Park, "Blockio Intelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," Futur. Gener. Comput. Syst., vol. 110, pp. 721–743, 2020.
[3] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT based food traceability for smart agriculture," in Proceedings of the 3rd International Conference on Crowd Science and Engineering, 2018, pp. 1–6.
[4] N. Kumar, S. Panda, P. Pradhan, and R. Kaushal, "IoT Based Hybrid System for Patient Monitoring and Medication," EAI Endorsed Trans. Pervasive Heal. Technol., vol. 5, no. 19, 2019.
[5] N. Kumar, S. N. Panda, P. Pradhan, and R. Kaushal, "IoT based E-Critical Care Unit for Patients In-Transit," Indian J. Public Health. Res. Dev., vol. 10, no. 3, pp. 46–50, 2019.
[6] https://ethereum.org/en/what-is-ethereum/
[7] Gustavo A. Oliva ·Ahmed E. Hassan · Zhen Ming (Jack) Jiang, "An exploratory study of smart contracts in the Ethereum blockchain platform" Published online: 12 March 2020, © Springer Science+Business Media, LLC, part of Springer Nature 2020
[8] A. Bahga, V. Madisetti, "Blockchain Platform for Industrial Internet of Things", Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016
[9] https://en.wikipedia.org/wiki/Blockchain/
[10] Julija Strebko Andrejs Romanovs, The Advantages and Disadvantages of the Blockchain Technology
[11] https://en.wikipedia.org/wiki/Smart_contract/
[12] https://arxiv.org/pdf/2001.06909.pdf
[13] J.Light, "The differences between a hard fork, a soft fork, and a chain split, and what they mean for the future of bitcoin" [online]. September 2017. Available from: https://medium.com/@lightcoin/the-differences between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean for-the-769273f358c9
[14] W. Fauvel, "Blockchain Advantages and Disadvantages" [online]. August 2017. Available from: https://medium.com/nudjed/blockchain advantage-and-disadvantages-e76d fde3 bbc0
[15] A. Bahga, V. Madisetti, "Internet of Things: A Hands-On Approach", Atlanta, 2014
[16] A. Songara, L. Chouhan, "Blockchain: A Decentralized Technique for Securing Internet of Things". Conference paper, October 2017
[17] Blockchain Technology, "Advantages & Disadvantages of Blockchain Technology" [online]. 2016. Available from: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages -disadvantages/
[18] J. Golosova, A. Romānovs, "Overview of the Blockchain Technology Cases". In Proceedings of the 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), October 10-12, 2018, Riga, Latvia. IEEE, 2018, pp.1-6. ISBN 978-1-7281-0098-2



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY