Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (6-13), Month: May - August 2023, Available at: www.noveltyjournals.com

Principles underlying the authenticity of Blockchain transactions

Professor KABEYA TSHISEBA Cedric

National Pedagogic University(DRC)

DOI: https://doi.org/10.5281/zenodo.7886085

Published Date: 02-May-2023

Abstract: **Blockchain, chain of blocks in French, is a technology that makes it possible to keep track of a set of transactions, in a decentralized, secure and transparent way, in the form of a chain of blocks. Developed from 2008, it is, first and foremost, a technology for storing and transmitting information. This technology offers high standards of transparency and security because it works without a central control body.**

More concretely, the blockchain allows its networked users to share data without an intermediary.

Everyone praises the efficiency of the blockchain which is indeed an exceptional transactional system, and more and more used as a cryptographic concept for the security of several types of transactions today, except that these same people extolling the said efficiency, do not do not know exactly the principles underlying this effectiveness, something that we have proposed to clarify in this article, in order to remove ignorance in this matter, thus affirming its relevance.

Keywords: **Authentication, Bitcoin, Blockchain, One Way Functions.**

1. INTRODUCTION

The notion of transaction can be defined in different ways. It can be considered as a commercial or stock market transaction, a contract, an agreement, or even, in computing, a basic operation of entering or consulting information. Several models exist today. However, all of them are based on certain characteristics: the two or more parties that make it possible to carry out a transaction, and a trusted third party, making it possible to certify the validity of this transaction. Since the birth of the notion of property, many transactions were noted in registers, and these documents were the physical proof of the authenticity of the transaction. Then the use of fiduciary currencies, which are no longer metallic coins, but notes, or paper possessing a certain value other than physical, obliges society to use institutions in order to guarantee the value of these new means of transaction. Thus, trust becomes, through the control of these institutions, a fundamental basis for any transaction.

The internationalization of transactions, from the post-war period, implies new transaction methods, the number of transactions increasing exponentially. The risk related to the authenticity of transactions is increasing and new trusted third parties are needed. For example, the SWIFT interbank system in 1977 or the WTO in 1995 were created to regulate transactions. These trusted third parties must allow transactions to be secured on the one hand, as well as a fluidity which would be the same for economic actors as if they were acting without institutions, thus not generating any economic loss.

With increasingly sophisticated technological advances, particularly in cryptography and network management, this model could be replaced by a new system. It could, among other things, eliminate the role of the trusted third party. However, these technological advances have been, for many people, the possibility of updating a pre-existing philosophy, advocating equality through the economy and technology in particular. Thus, the ideology of this new technology, called Blockchain, is the heir to “Cyberpunk” ideologies, which see technology as a means of breaking free from unequal human control.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (6-13), Month: May - August 2023, Available at: www.noveltyjournals.com

This research aims to present the transaction system based on Blockchains, especially the principle underlying the operation of the authenticity of transactions (trusted third party).

2. INTRODUCTION TO BLOCKCHAINS

The purpose of this part is to present blockchains in a conceptual way at first, before then specifying the technical mechanisms related to this technology, based on the creation of the first blockchain: that of Bitcoin. The Blockchain is a chain of blocks of computer codes. Each block contains attributes relating to one or more transactions (sender, recipient, amount, etc.), or other objects that will be specified later. It also contains information related to the predecessor block on the Blockchain, and it is encrypted, i.e. it is secured using cryptographic processes (computer algorithms). When recent transactions are recorded, they are grouped into blocks, and each transaction will be validated by the "miners", who will analyze the entire blockchain.

3. TECHNICAL DETAILS STARTING FROM THE ORIGIN OF BLOCKCHAINS: BITCOIN

3.1 Introduction

In order to better understand the technical functioning of the Blockchain, we will focus on the underlying system of Bitcoin, explained by Satoshi Nakamoto, in his publication "Bitcoin: A Peer-to-Peer Electronic Cash System", available on the website www. bitcoin.org.

First of all, Bitcoin is a cryptocurrency invented in 2008, and whose open source software was released in 2009. A cryptographic currency, or cryptocurrency, is electronic money on a Peer-to-Peer or decentralized network (each client, called node, is also a server). In order to secure this currency, the transaction system is based on the blockchain concept, based in part on cryptographic processes.

Satoshi Nakamoto's intention was to create an electronic payment system, which could do without the intervention of financial institutions. Nowadays, online commerce is dependent on financial institutions. These institutions aim to perform payment processing. However, this system has weaknesses, including in particular that of having to place one's trust in these said institutions. For example, a purely irreversible transaction is not possible in this system, since the institution manages conflicting transactions. In addition, these institutions have an operating cost to carry out this mediation work. This cost therefore affects the transactions carried out, thus preventing the possibility of carrying out low-cost transactions. These two issues, which are irreversibility and cost, are two major challenges for this technology. The possibility of transaction reversal for an irreversible service generates an additional cost. This requires increased trust, required supporting documents, and the possibility of having a non-zero risk of fraud. It is therefore, for Satoshi Nakamoto, to allow the use of a virtual currency, limiting the problems set out above.

It thus proposes a system based on cryptographic proofs, supposed to replace the confidence granted to financial institutions. This system aims to meet several challenges:

A transaction between two parties without a trusted third party

Sellers protected against possible fraud thanks to the impossibility of deleting or modifying a transaction - Buyers protected with a system of escrow accounts (legal term: unavailability of an asset for a short period)

No double spending possible thanks to the time stamping of transactions

This system is however only possible if the computing power of the "honest" nodes of the network is greater than that of the nodes acting to carry out a combined attack on the network. This concept will be explained later.

3.2 Transactions

An electronic document is defined as a chain of digital signatures. An owner can transfer this part in this way:

1) Verify and digitally sign the fingerprint / hash of the previous transaction (1 and 1')

2) Verify and digitally sign the new owner's public key (2)

These signatures are added at the end of the transaction (3). Recipients have the option to verify the chain.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (6-13), Month: May - August 2023, Available at: www.noveltyjournals.com

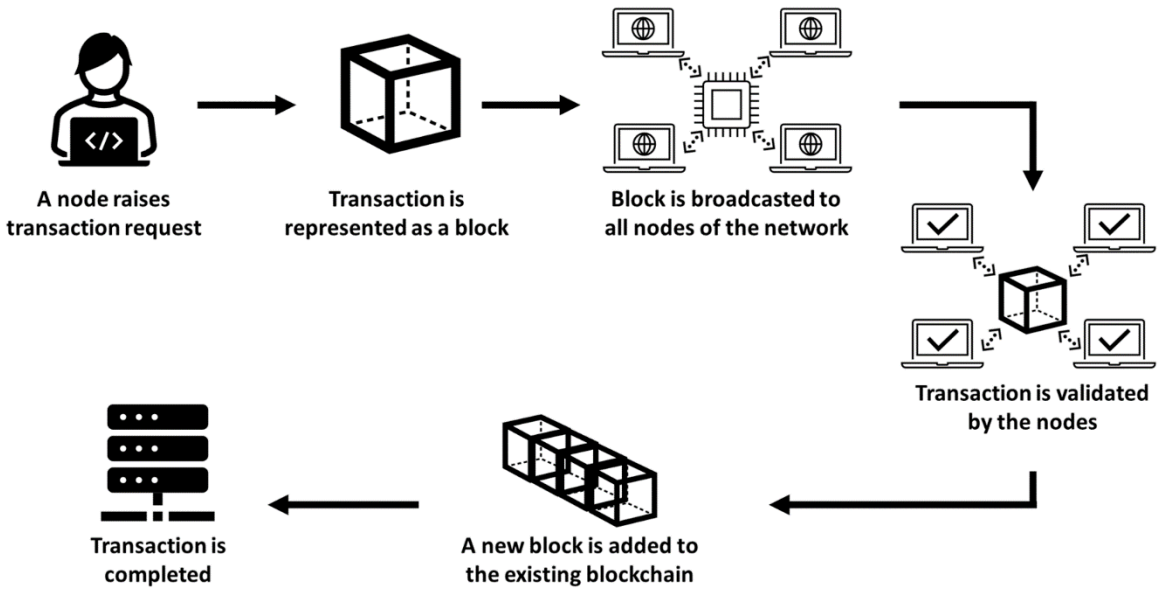

Fig1. Blockchain transaction system

This system alone raises a major problem in particular: a beneficiary cannot check whether a previous beneficiary has made a "double spend" with the coin. One solution could be to create a transaction monitoring authority, or trusted third party. Thus, each piece should be returned to this authority, which creates a new one. Only parts from this entity are then accepted. This prevents a room from being used twice. However, this solution relies on this trusted third party. This is precisely what Satoshi Nakamoto wanted to avoid.

In the case of the trusted third party, the latter was aware of all the transactions carried out, which allowed him to know whether a coin had been used in another transaction or not. A reliable and efficient method to know the history of all transactions in a shared way must therefore be found. Of all the new transactions involving this electronic coin, only the oldest must be the one that the system must validate. All transactions must therefore be made public, and the system must ensure that all its participants show a common history of transactions. The beneficiary therefore needs to know that the majority of the nodes have established this history (condition which validates the block of transactions), and this for each transaction time.

The concept of transactions is actually based on asymmetric cryptography. The latter links two key elements: the public key and the private key. They make it possible to guarantee the integrity of the data transmitted by encrypting the data sent, as well as the authentication of the origin of the transaction.

When someone embarks on the process of creating a transaction, they generate, using dedicated software, a public key and a private key. The private key is not transmitted to anyone and the public key is available to everyone.

4. KEY PRINCIPLES OF A BLOCKCHAIN

In the previous paragraph, we explained the technical functioning of a particular blockchain, which is that of Bitcoin. However, each blockchain works with different processes, different security methods. We will therefore attempt, in this paragraph, to summarize the main technical principles that govern a blockchain, and what is likely to be modified. For this, we will take each step of the explanation of the Bitcoin blockchain and draw the synthesis. We will also illustrate the differences between the bitcoin blockchain and other blockchains using examples.

Thus, we can state all the key principles on which the Bitcoin blockchain is based. These principles are:

Definition of transactions

Validation steps by the network (including time stamping and proof of work)

Miners reward

Privacy

In the following sections, we will look at each of these elements by detouring the principles inherent in any blockchain.

4.1 Many objects usable by the blockchain concept

The type of objects of a blockchain can be varied according to its nature. The object deposited on a blockchain can also be other than a transaction (object in the Bitcoin example). The best-known example is undoubtedly that of smart-contracts.

A smart-contract is a computer program inserted into a block that runs when certain conditions are met, or certain events occur. This implies that the blockchain system must make it possible to collect information that may be outside the blockchain, and which ensures the conditions of a contract.

We can for example imagine a person who chooses to give 1 btc to his brother when the latter becomes a father. Thus, a smart contract can be generated. A smart contract is linked to an account. There are two types of account:

Accounts held by third parties, which are controlled and secured via private keys

Contract accounts, controlled and secured only by their code

A third-party account can only perform a transaction "manually", i.e. using its private key. On the other hand, in the case of a contract account, each time the latter receives a message, its code executes and its functions apply. This can create a new contract, generate a transaction or call another contract.

Thus, in our example of donating a btc to his brother, it is necessary, to fulfill the conditions, to verify that the brother of the creator of the smart contract has a child or not. It therefore requires an entity, external to the blockchain, which deposits the information at a pre-established address (the content of which will be checked with each message sent to the address of the smart contract). This entity is called Oracle.

Indeed, due to the immutable characteristic and taking into account the need for security of the blockchain, the latter does not have the possibility of interacting with external elements. On the other hand, an external entity can generate a “transaction” on the Blockchain. In our example, the oracle, which is an external organism, automated or not, can search on a database of births if the brother has a child. The oracle may very well also be a third party, or the creator of the smart contract. It all depends on the code itself. He will then write the result of his search to the address provided, which will condition the result of the smart contract.

The principle of the oracle and the smart contract can be schematized as follows:

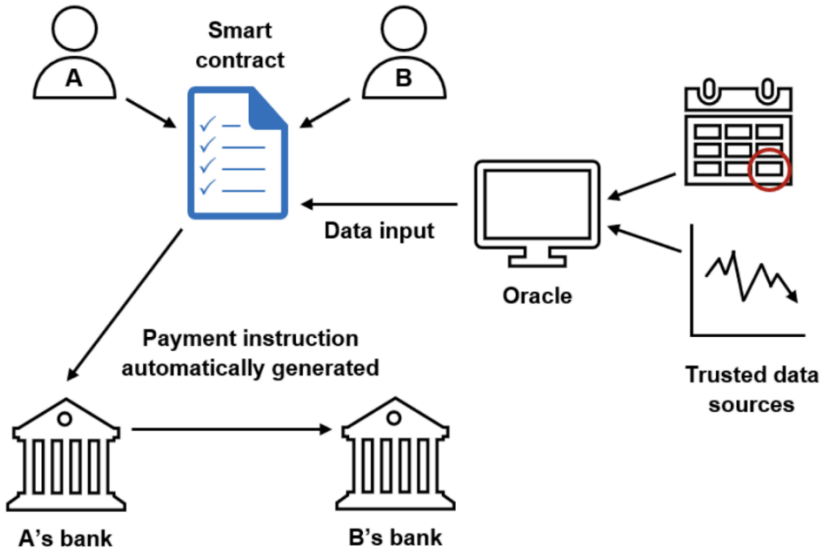

Figure 2: Illustration of the smart contract example

We see here that the result of the smart contract depends mainly on the information provided by the oracle. Indeed, if the oracle decides to give bad information, the smart contract will be executed taking into account this erroneous information. Similarly, if the oracle does not deliver any information to the address indicated in the code of the smart contract, then the conditions of this contract will never be fulfilled. Thus, the system relies again on a trusted third party.

Several structures have thus been devised in order to deal with the problems linked to the introduction of oracles into the blockchain ecosystem:

In the event that the necessary data is available on a server, organizations offering so-called "provable-honest" services offer to search for the requested data, accompanied by proof of its validity. For example, the company Oraclize, which operates in particular on a blockchain called Ethereum (whose cryptocurrency is ether) operates according to the following scheme:

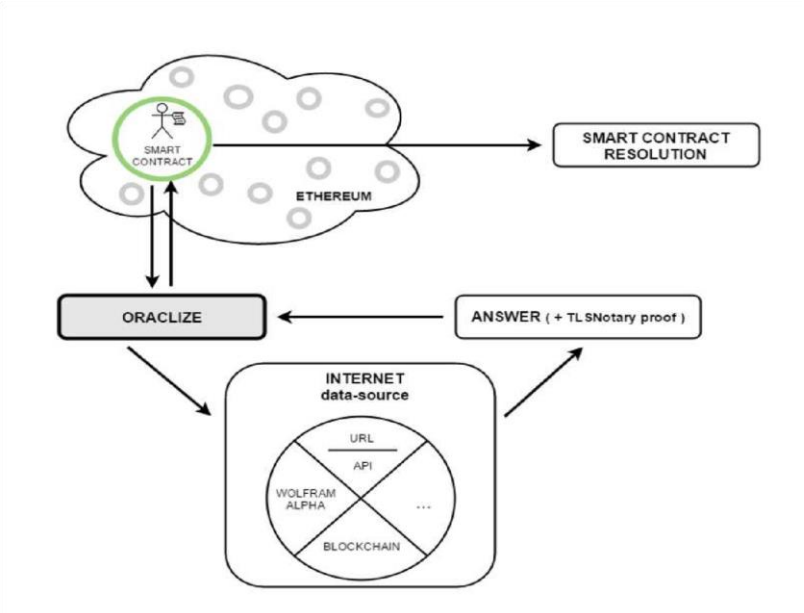

Figure 3: Operation of Oracle (source: https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-etle-monde/)

In addition to the data, Oraclize delivers a "proof of honesty" which makes it possible to know whether the data is indeed that available on the server. This data being deposited on the blockchain, it is easily verifiable. Thus, if the oracle gives erroneous information, the reputation of the oracle will be at stake. It is therefore on the reliability of the oracles that this type of organization is based.

There are also consensus-based oracles. This is a principle similar to that of a vote. The information required by the smart contract is requested from a large number of participants, who are encouraged to give the correct answer (by a reward system for example). This system is decentralized, and in essence, perfectly compatible with a blockchain system.

We can also cite physical oracles. Some information can be collected automatically from physical data. We can imagine a temperature sensor, and a smart contract linked to it. To go further, one could imagine a set of physical sensors that can, in some way, detect a localized disaster. Thus, a smart contract could directly compensate an insured who has subscribed to this contract.

One can also find on the blockchain specific organizations, called DAO for Decentralized Autonomous Organization, which are autonomous entities. We can illustrate the principle of these entities by an example. An entity such as this could, for example, provide a new type of insurance service. All participants in this organization could pay monthly installments to this organization through smart contracts. When one of the participants suffers an accident and wishes to be compensated, he makes a request. Either the smart contract relies on oracles capable of confirming the claim, and thus automatically compensates the insured, or the compensation is submitted to the vote of all the insured, who decide whether or not the

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (6-13), Month: May - August 2023, Available at: www.noveltyjournals.com

insured can receive compensation. Thus, each participant can have decision-making power over the actions of the smart contracts. Thus, the governance of an application such as a DAO depends on the smart contract(s) that have been coded.

4.2 Network validation steps

In the description of the validation steps by the network, in the case of Bitcoin, the Proof of Work step makes it possible to create a consensus between all the nodes of the network to establish the valid history of transactions. This helps to prevent possible malicious attacks, and to choose a branch when two are created. The proof of work is mainly based on the fact that it is necessary to prove that enough energy and computing resources have been used. However, this method is not the only one offered by blockchain creators.

Another popular method, which is not the one explained in Satoshi Nakamoto's paper, is called Proof of Stake. This method relies on having cryptocurrency.

Let’s compare these two methods to better explain proof of stake:

- Proof of Work: imagine that each node has the same computing power as the others. Each node rolls a die at the same frequency as the others to get the desired number (imagine a 6). When a node rolls a 6, it tells everyone else, and its block is added to the chain. Thus, whoever has the most nodes has the best chance of success. Now, if the nodes have different computational powers, the one who owns the nodes, which, cumulatively, have the most power, will have the best chance of success (it's like increasing their frequency of throwing) . We can conclude that the chance of being the miner who successfully adds a block is theoretically proportional to the computing power possessed.

- Proof of Stake / Proof of Stake: in the same way, the concept of this method is that the success of obtaining the mining of a block depends proportionally on the money that one has on his account. For example, if an account has 10% of the total currency in the system, then it will have a 10% chance of offering the block to be added first. This method has the advantage of consuming much less energy, however it is known to be less secure than Proof of Work.

There are many other types of evidence, each with advantages and disadvantages. They will not be presented here.

Other differences are also remarkable, such as the generation time of a new block (12 s for Ethereum against 10 min for Bitcoin).

4.3 Reward of minors

In the case of Bitcoin, the rewards are halved approximately every 4 years. This principle is not the case for all blockchains. Ethereum rewards in the same way every year all the miners who participated in the addition of blocks, and this forever (15.6 million ether are generated every year).

4.4 Confidentiality

The original concept of the blockchain included validation taking into account all the nodes of the network. Among other things, the blockchain itself, as well as the validation of the blocks that constitute it, was carried out in a totally shared, and therefore public, manner.

Some institutions, interested in this new technology, have however been suspicious of the public nature offered by the blockchain in its original state.

New concepts have thus emerged, following this identified need. These are “private” or “consortium” blockchains.

A consortium blockchain is a blockchain based on a block validation process that is restricted to a certain number of defined nodes. The ability to read the entire blockchain can be reserved for certain particular nodes, the consultation will therefore be private; it can also be available for all nodes, in which case the consultation of the blockchain is public. The blockchain can also be separated into several parts: some data can be consulted publicly, while others are only available on a private network, the consultation is, in the latter case, hybrid.

A private blockchain, on the other hand, reserves the validation process to a single actor, the consultations being able to be private, public, or hybrid.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (6-13), Month: May - August 2023, Available at: www.noveltyjournals.com

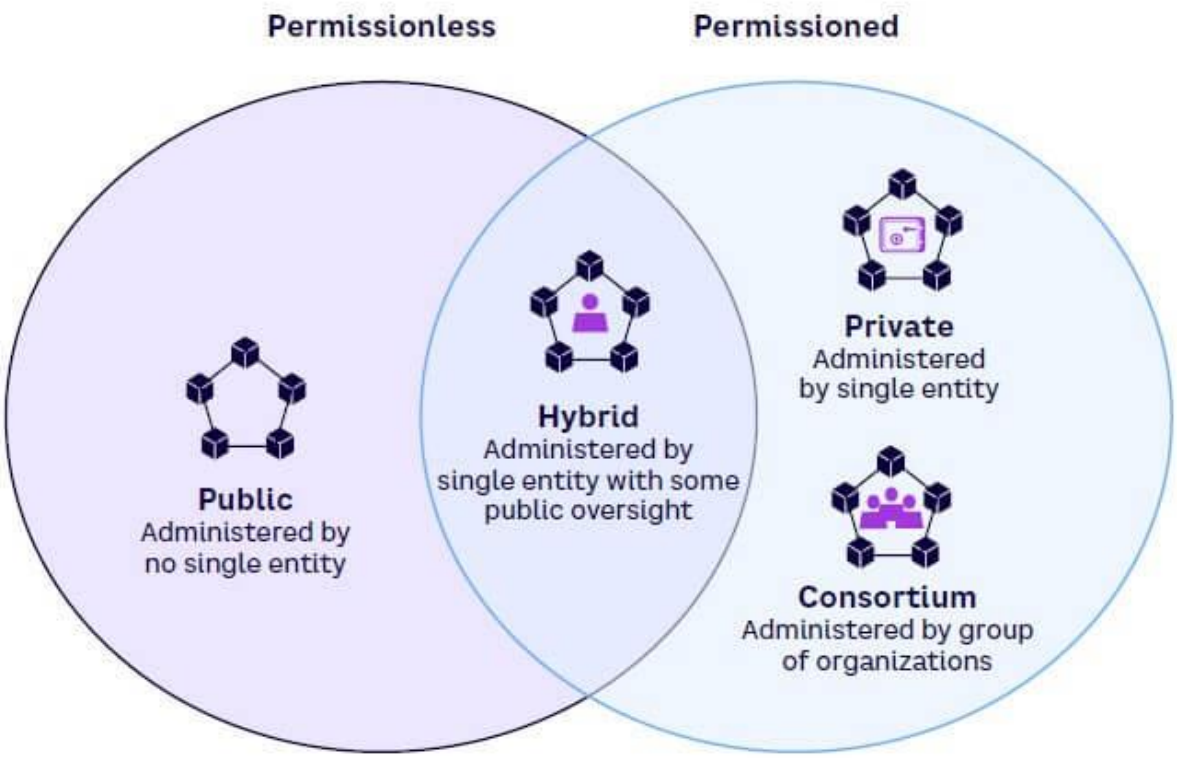

Figure 4: Blockchain types by block validation mode

5. CONCLUSION

In this document, we were first able to study the technical process on which the Blockchain is based. This IT innovation thus makes it possible to organize data exchanges on a distributed network, ensuring data security by encryption, and involving the nodes of the network for the creation of new blocks in the chain.

We saw in a second part what this technological innovation induces, in terms of potential changes, in different sectors of activity, and we tried to extract the key elements that make the blockchain a disruptive invention.

Despite everything, the blockchain is in a phase of peaks of expectations, and has begun to experience some disappointments. Indeed, the Ethereum blockchain was “attacked” in June 2016. The reason for this flaw was an unverified code contained in a smart contract. However, several times a year since its inception, articles predict the end of Bitcoin in the coming months, and the Bitcoin blockchain has, until today, experienced no disappointment. Thus, we can conclude that the confidence in this new technology is not complete, and that it needs more experience and initiatives in order to make it viable in the business world.

This technology is therefore faced with several challenges:

Knowledge of the blockchain principle is essential. This notion is now widely used as a “buzz word”, and few understand with finesse the technical cogs on which the blockchain is based. This issue requires a popularization of terms that are today too technical for a public uninitiated in computer science.

One of the principles of the blockchain is based on a sufficiently provided network to be able to grant a certain confidence to the network. Thus, blockchain technology must be the subject of sufficient support to ensure its proper functioning. • Blockchain initiatives are very numerous and dispersed. As with most other computer technologies, blockchains must meet standards in order to ensure that it operates as normal. These standards are not yet fully established and standardization is necessary. • Some particular use cases lead to sustained disputes between experts. This can lead to divisions among the most knowledgeable members of this technology. These squabbles can work against blockchain's buy-in from prospective decision makers.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (6-13), Month: May - August 2023, Available at: www.noveltyjournals.com

REFERENCES

[1] Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. Comput. Ind. Eng. 2019, 135, 582–592. [Google Scholar] [CrossRef]

[2] Emerge Stronger at a Time of Uncertainty: Blockchain for Supply Chain, Forrester Opportunity Snapshot: A Custom Study Commissioned by IBM. 2020. Available online: https://www.ibm.com/downloads/cas/JX9KDGPJ (accessed on 10 November 2021).

[3] Aslam, J.; Saleem, A.; Khan, N.; Kim, Y. Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. J. Innov. Knowl. 2021, 6, 124–134. [Google Scholar] [CrossRef]

[4] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 November 2021).

[5] Lamport, L. The part-time parliament. ACM Trans. Comput. Syst. 1998, 16, 133–169. [Google Scholar] [CrossRef]

[6] Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfede, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction; Princeton University Press: Princeton, NJ, USA, 2016. [Google Scholar]

[7] Kumar, R.; Khan, F.; Kadry, S.; Rho, S. A Survey on blockchain for industrial Internet of Things. Alex. Eng. J. 2022, 61, 6001–6022. [Google Scholar] [CrossRef]

[8] Denny, D.M.T.; Paulo, R.F. Blockchain and the Agenda 2030. In Blockchain Technology and Applications; Nova Science Publishers: Huntington, NY, USA, 2019; p. 230. Available online: https://novapublishers.com/shop/blockchain-technology-and-applications/ (accessed on 10 November 2021).

[9] Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 2016, 11, e0163477. [Google Scholar] [CrossRef] [PubMed]

[10] Swan, M. Blockchain, 1st ed.; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015; ISBN 9781491920497. [Google Scholar]