Blockchain: A Disruptive and Transformative Technology of the Fourth Industrial Revolution

Mark J. Mwandosya[1] and Matthew L. Luhanga[2]

ABSTRACT

The blockchain, a technology that is variously described as Web 3.0 or the internet of value, is expected to play a disruptive and transformative role in the Fourth Industrial Revolution (4IR). As a digital platform, it is disrupting legacy business models and creating new ones. While much work is currently being undertaken on the advances and utilization of this nascent technology, there is a paucity of scholarly output, particularly from African centers of learning. This paper describes the evolution and development of the technology, its positive elements, and barriers to its application. Suggestions are made on opportunities available to African centers of excellence for carrying out research, consultancy, and curriculum development in new business models. National policies are essential in order to provide contexts for blockchain and related 4IR technology development and utilization.

Key words: *blockchain, cryptocurrency, digital currency, distributed ledger technology.*

INTRODUCTION

The First Industrial Revolution (1IR) came about with the advent of the steam engine. It was characterized by mechanization and weaving looms (textile industry). Later on, the discovery of electricity led to mass production facilitated by the assembly line. Electricity was to underpin the Second Industrial Revolution (2IR). Electricity has led to the development of electronics, computers, and automation. These technologies are the foundations of the Third Industrial Revolution (3IR) (Schwab, 2016). The Fourth Industrial Revolution (4IR), a term first coined by Klaus Schwab, is an extension of the 3IR in the creation of cyber–physical space brought about by the interaction among digital, physical, and biological systems (Schwab, 2016). Technologies for the 4IR include genetic engineering, materials technology, nanotechnology, biotechnology, and information and communication technology which embrace quantum computing, 5th generation wireless technology, internet-of-things, 3D printing, and distributed ledger technology (DLT) – a broad category that includes blockchain technology. The blockchain, a technology that is variously described as Web 3.0 or the internet of value, is expected to play a disruptive and transformative role in the Fourth Industrial Revolution (4IR). It is disrupting legacy business models and creating new ones. The importance of blockchain technology is manifested in its use in facilitating the management of data in a decentralized manner and without intermediation, such that contributors of the data, nodes in a network, do not need a central dedicated and trusted node, through which, ordinarily, transfer of data would take place (Rosic, 2019). We describe below, the evolution and development of the technology, its positive elements, and barriers to its application. Suggestions

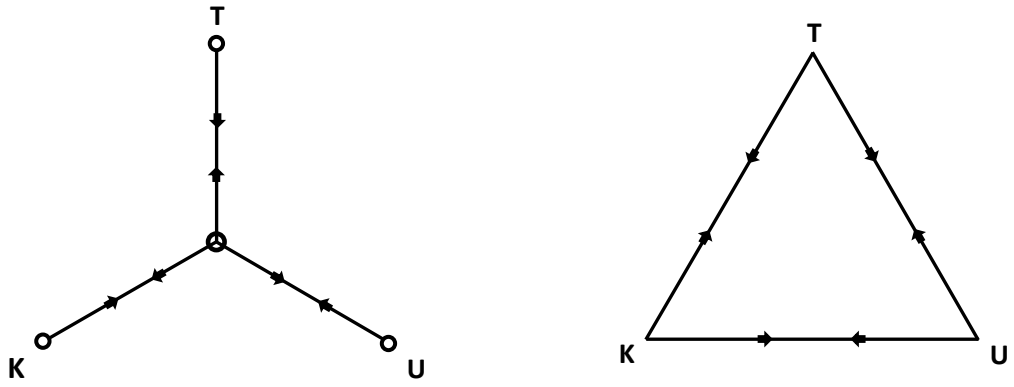
[1] M. J. Mwandosya -Fellow of the Institution of Engineers Tanzania (IET), Fellow of the Tanzania Academy of Science (TAS), Registered Engineer (Reg. Eng.), Founding Chancellor Mbeya University of Science and Technology. {Corresponding author's email: mjmwandosya@gmail.com)
[2] M. L. Luhanga -Fellow of the Institution of Engineers Tanzania (IET), Fellow of the Tanzania Academy of Science (TAS), and a Registered Engineer (Reg. Eng.), 5th Vice–Chancellor, University of Dar es Salaam.
Business Management Review: Volume 23, Number 2, Pages 16-31, ISSN 0856-2253 (eISSN 2546-213X) July-December, 2020 UDBS.

are made on opportunities available to African centers of excellence for carrying out research, consultancy, and curriculum development.

BASIC CONCEPTS

To illustrate the concept of decentralization and disintermediation in a very simplified manner, consider an individual T, wanting to send t shillings to individual U. U wishes to send u (u<t) shillings to individual K. T has to use a bank as an intermediary connecting T and U. The bank, through a corresponding bank has to be satisfied that U does indeed exist and can be availed of the money sent by T. Intermediation is a process that creates trust among T, U, and K. However, the transfers are made at the cost of time and money. For "U" will receive an amount u-s where "s" is the service charge due to the bank. Furthermore, intermediation and transfer may take days to weeks. The transactions illustrated in Figure 1 (left) are executed with the control of an intermediary.

Figure 1: Basic Illustration of Centralized (left) and Distributed Ledger (right)



A new concept has emerged that disrupts the traditional mode of transfer by doing away with the intermediary. The system works as follows: T will indicate the intention to transfer t shillings to U. That information will be stored as data available to T, U, and K simultaneously. The participants will all verify that T indeed has an amount t that has to be transferred to U. That information in data form creates the first block say. U's transaction forms the second block linked to the first block. Likewise, the participant K transaction will form the third block, to be added to the previous blocks. The linked blocks form what could be conceptualized as a chain of blocks or blocks linked by chains; hence the name blockchain.

In reality, T, U, and K represent three of what could be a large number of linked computers. The entry of data into one, through the creation of a block, is simultaneously available to each participating computer (nodes). The nodes are anonymous. Once the data is entered, and a block is formed, there is no way that data could be changed or hacked. For that to happen, all the participating computers in the network must concur with the change. The blockchain information is available to each computer such that intermediation (trust) is rendered unnecessarily. The structure of the blockchain and the transparency of the network, provide the necessary safeguards.

Consensus Seeking (The Byzantine Generals Problem)

In the absence of intermediation, participating computers or nodes in the network require some form of reaching a consensus in communication. This is a classical challenge in computer science and communication and is referred to as the Byzantine Generals Problem, initially formulated in a

pivotal paper by Lamport, Shostak, and Pease (1982). The problem is described figuratively in terms of four or any number of generals of a Byzantine army surrounding a garrison town which is heavily defended. The town can fall only if the generals agree to spring a coordinated attack at an exact time. For this to happen, two conditions are required; secure communication and the absence of a traitor or traitors among them. One general can initiate communication spelling out the day and time for the attack. A messenger has to deliver the same to the other generals. Four things could happen to the courier. Firstly, he may fall into the enemy camp and be eliminated, in which case no message would reach the other generals. Secondly, he may be compromised and made to tamper with the message, sending the wrong message to the generals. Thirdly, he may just lose the message. Fourthly, he may succeed in his mission and deliver the message. However, a dishonest general may temper with the message and forward it to other generals with the day and time of attack altered. The confusion arising is that some generals may launch the attack some may not, with disastrous consequences on the part of the Byzantine army (Kwatra, 2017; Massessi, 2018).

The corollary to the Byzantine Generals Problem is that each general represents the node of a distributed network. Messages are akin to transactions. Maliciously acting nodes represent the enemy garrison town; faulty communication is results from traitor messenger action. Participants of a distributed network need to agree on the current status of the network in the absence of central intermediation, and must be assured of the security of information exchange in an ecosystem that has dishonest actors.

A Byzantine Fault Tolerance is the property of a system to resist failures that result from a Byzantine Generals Problem. A Byzantine Fault Tolerant system is the ability of a system to operate in a situation where some nodes fail to operate or act maliciously, in a corrupt or hostile manner (Massessi, 2019). Blockchain technology, through the application of cryptography, mathematics, and computing solves the Byzantine Generals Problem using consensus mechanisms.

Origin of blockchain

The blockchain is conceptually based on an old method of book-keeping using the ledger. One of the most challenging tasks in any work is how to keep a time-stamp (a mark in form of time) to avoid double-spend, forgery, or to confirm ownership of written material, discoveries, and other important works such as patents, and to certify when a document or record was first created, changed or modified. Electronic digital documents are prone to being tampered with. In a seminal paper titled: “How to Time-Stamp a Digital Document”, Haber & Stornetta 1991 conceived the idea of using cryptographic hash functions to link the steps used in a document time-stamping process. The essence of their work was to implement a system by which document time-stamps could be tamper-proof. This concept was further improved in 1992 when the Merkle Tree was incorporated in their design to reduce the storage space and computational load required in the validation steps of the time-stamping process (Bayer et al., 1992).

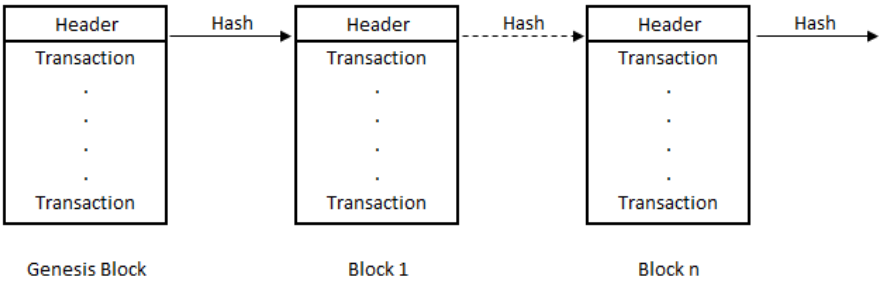
The concept of the blockchain was further developed, improved upon, and popularized by Nakamoto (2008), who in his/her or their white paper – “Bitcoin: A Peer-to-Peer Electronic Cash System” - extended the concept of immutable time-stamping of documents to a peer-to-peer (P2P) coin-based payment system. Transactions in the payment system were aggregated into blocks and the blocks were then cryptographically linked into a *blockchain* as shown in Figure 2. The payment system also solves the problem of double-spend (Nakamoto, 2008). Double-spend is a problem

that arises from a situation where an individual A has x shillings only. He or she gives B, x shillings, and attempts to give C the same x shillings. While in physical money that would not be possible, the existence of funds digitally in a computerized ledger is such that it is possible to tamper with it and spend the money twice or more times. In a decentralized payment system whereby a copy of the ledger is available to all participants, who must agree to any addition or change in the ledger, the double-spend problem is solved.

Satoshi Nakamoto, an anonymous person or group of persons, through their seminal paper, has/have opened up the new field of cryptocurrency, and the use of blockchain technology, in applications which require transparency, auditability, resiliency, and seamlessness, and does not require trust in the management of large amounts of data (Nakamoto, 2008). The necessary safeguard is assured through cryptography, an old practice whereby a message is encrypted in such a manner that it is unintelligible to a third party. It protects the integrity and secrecy of information so that only those, for whom it is meant, can process, decipher, and read the information. Cryptography, originally a science of message encryption, has grown into a field in its own right, based on mathematical theory and computer science. Cryptography is about confidentiality, integrity, non-repudiation, and authentication of information. Two key aspects of cryptography in blockchain technology are hashing, and the application of public and private keys (Decent, 2019).

To appreciate this new and emerging technology, Blockchain should not be confused with Bitcoin. Blockchain is the technology which has enabled transactions of the Bitcoin, and numerous other cryptocurrencies that have come into being.

Figure 2: The Blockchain



Hashing

Information contained in a block has to be formatted in such a manner that it cannot be interfered fraudulently or in any other corrupt or pervert manner. This reliability is assured through hashing, a process by which information or data is cryptographically encoded using a mathematical algorithm such that an input of any length is turned into a fixed–length output (Nelson, 2018). In such a situation, decrypting the output data to work out the original data is virtually impossible (Fortney, 2019). A hash function has the following characteristics (Drescher, 2017): the hash value (output) changes unpredictably when the input data is changed. It is therefore, pseudorandom. Input data cannot be recovered from the hash value. It is a one-way function (It is said to be *preimage resistant)*. Identical input data yield identical hash values; and, the possibility of different data sets resulting in identical hash values is negligible. This is due to hashing functions being *collision resistant*.

Hashing in the Bitcoin network is used for several purposes. First, it is used to create identifications of transactions. The hash of a transaction yields a Transaction ID (TXID). Second, hashing is used

to create identification for blocks of a blockchain. Each block of a blockchain is identified by the hash of the block's header. This is called the *block hash.* The structure of the block header is shown in Figure 3. In Figure 3, the hash names are taken from the Bitcoin Core Reference Client (Bitcoin Core Developer Reference, n. d.). The prefix n indicates that the fields are integer variables.

Figure 3: The Block Header Fields

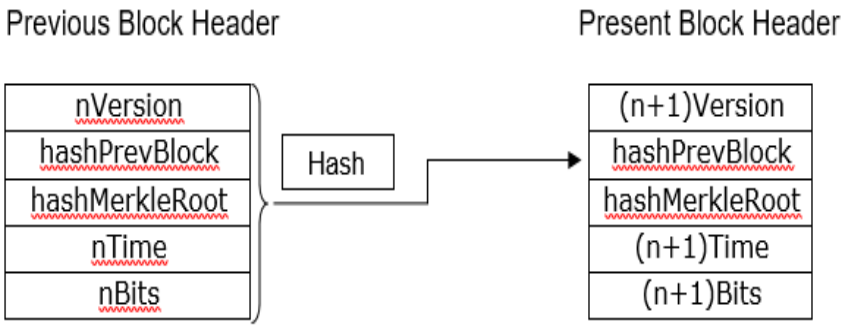
nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

Source: Bitcoin Developer Reference, n.d.

The fields in the block header represent the following: The nVersion field stores the current version of the block; the hashPrevBlock field in the block header contains the block hash of the previous block in the blockchain; the hashMerkleRoot field stores the hash of the transactions in the block; the nTime field stores a time-stamp in Unix time format to record the time of the creation of a block in total seconds counted from the Unix epoch, 00:00:00 Thursday January 1st 1970 and in which every day is 86400 seconds long; and The nBits field which stores the current *target hash.* The miner who is the first to create a hash that is less than or equal to the target hash succeeds in adding the next block to the blockchain. In cryptography, the word nonce is used to denote a number that is used only once. A miner sets a nonce in the current nNonce field. The block header is then rehashed. The process is repeated until the solution meets the restriction, that is, the resulting hash is less than or equal to the target hash.

The block hash of the previous block occupies the hashPrevBlock of the current block and, since the process is recursive, this generates the blockchain linking all blocks from the genesis block up to the current block. This linking is depicted in Figure 4.

Figure 4: Linking of Blocks in the Blockchain



Source: Bitcoin Developer Reference, n.d.

Public and Private Keys

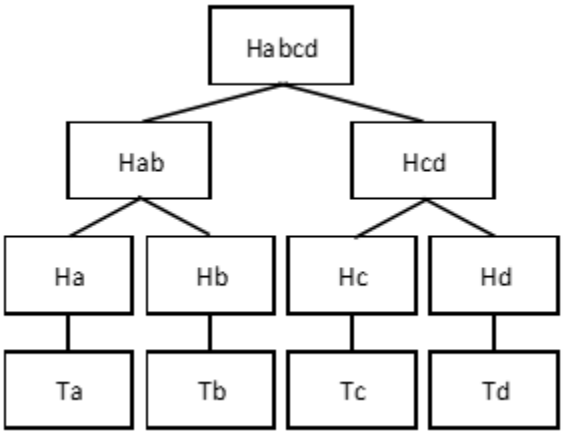
Elliptic Curve Cryptography is used in blockchain technology (Anoop, 2018). Messages and transactions are mathematically encrypted such that a user has two keys; the private key and the

public key (IHODL, 2018). The private key is used to sign a message or transaction. It is akin to a password. It is only the signatory who is supposed to know the key and guard it secretly. The public key is made available to every user or node in the peer network. Sharing of the public key does enable other users or nodes to confirm or verify that the message came from the person who has signed the transaction. Put simply, person X would sign a message or transaction to person Y using X's private key and Y would use X's public key to confirm that the message or transaction came from X.

Merkle Tree

The Merkle tree is made up of leaves, branches, and the root, like a tree, visualized upside down. Each leaf node could be considered to represent a transaction. The hash of a transaction forms the first non-leaf or branch node. Subsequent or upper non-leaf nodes are hashes of upper branch nodes. The exercise is repeated by hashing pairs of lower hashes until only one hash, the root hash, or the Merkle Root is left at the highest point (Ray, 2017).

Figure 5: Illustration of a Merkle Tree



Source: Gardner, 2018

Figure 5 shows the Merkle Tree in its simplest form. Let Ta, Tb, Tc, and Td be separate transactions and Ha, Hb, Hc, and Hd represent hashes of Ta, Tb, Tc, and Td, respectively. These hashes would themselves be joined together and hashed into a pair, Hab and Hcd. These two hashes are combined and hashed to form the root or Merkle root hash Habcd. The root hash or the Merkle root stored in the hashMerkleRoot field of the block header represents a summary of the data representing all transactions (Gardner, 2018).

The Bitcoin network contains two types of nodes; full nodes and *simple payment verification* (SPV) nodes. Full nodes store whole blocks whereas the SPV nodes store only block headers. When SPV nodes need to verify the membership of a transaction in a block, they consult full nodes which respond with information which, in combination with information in the hashMerkleRoot field of the SPV node's header, enables the SPV node to verify the membership of a transaction (Bitcoin Developer Reference, n. d.).

Consensus Mechanisms

In a blockchain, multiple players are involved. For the blockchain to self-regulate, a reliable and secure mechanism is required to make sure that transactions being added to the blockchain are genuine to the satisfaction of, and with the consensus of, all or the majority of the players. Such a

network of nodes has been described above as a Byzantine Fault Tolerant system. The consensus mechanism sets the rules that determine the contributions of various players in updating the status of the distributed system (blockchain). There are many consensus protocols for blockchains and they differ depending on whether the blockchain is permissioned or permissionless (Baliga, 2017). We mention three protocols only.

Proof-of-Work (PoW) is one such consensus protocols. The PoW protocol allows thousands of anonymous and completely untrusting participants to agree on the status of an updated blockchain. The PoW protocol is used in the *mining* of bitcoins by network nodes called *miner nodes*. Through mining, new blocks are added to the blockchain. Each block that is added to the blockchain is identified by its *height.* The height of a block in a blockchain is the number of blocks preceding it. The genesis block has height zero (0). Suppose a miner node intends to create a candidate block for addition to the blockchain at height N, the hashPrevBlock field of the candidate block will be populated by the block hash of the block at height N-1. The hashMerkleRoot field of the candidate block will be populated by the Merkle root of the transactions in the candidate block. The nTime field will record, in Unix time format, the timestamp of candidate block creation. The goal of the miner nodes is to iteratively choose values from the nNonce field to create candidate blocks and search for a block whose block hash is less than or equal to the target threshold. A miner who successfully finds such a block is said to have *mined a valid block* which is added to the blockchain at height N. He/she is rewarded with newly minted bitcoins. The reward is called the *block subsidy.* The miner also receives *transaction fees* in bitcoins which are provided by the transactions in the block that is successfully added to the blockchain. The sum of the *block subsidy* and *the transaction fees* is the *block reward* (Bitcoin Developer Reference, n. d.).

Adding a valid block to a blockchain (mining) involves the solution of a computational problem, a Proof-of-Work algorithm, which is an iterative search through a large number of candidate block hashes. Mining involves the use of specialized hardware, *Application–Specific Integrated Circuits* (ASICs) for solving the PoW algorithm. The high computation and hardware costs make mining very costly and a preserve of those who can afford, motivated by the high returns. For a PoW system, on average, one block is added to the blockchain every 10 minutes. The number of transactions per second (TPS) is 3.

In creating the bitcoin source code, Satoshi Nakamoto decided that the block subsidy would be 50 bitcoins per block for the first 21000 blocks (Vijayakumaran, 2017). The decision to limit the number of blocks to be mined, just like in conventional mining, was meant to avoid inflation. Since a new block is added every 10 minutes, it takes approximately four years to mine 210,000 blocks. The block subsidy was halved for mining the next 210,000 blocks and is halved progressively for each of the next 210,000 blocks. From July 2016 to date, the bitcoin subsidy has been 12.5 BTC and was halved to 6.25 in May 2020. The smallest indivisible unit of the bitcoin currency is a *satoshi* whereby a bitocoin equals 10^8 satoshis. As the block subsidy is progressively halved, it will eventually become less than 1 satoshi. This is expected to occur around the year 2140.

Proof-of-Stake (PoS), of which there are many versions, is another consensus algorithm (Baliga, (2017). PoS systems have been designed to overcome inefficiencies associated with PoW systems regarding computational, energy, and hardware costs. There is no mining in PoS systems. A PoS system gives preference for adding the next block to a blockchain to those with more cryptocurrency coins.

Delegated Proof-of-Stake (DPoS) is yet another consensus mechanism, an alternative to PoS. There is no mining associated with DPoS systems. The special feature of DPoS is that participating nodes vote to elect *delegates, orwitnesses* who are responsible for generating and adding blocks to the blockchain. The number of *delegates* is that which satisfies at least 50% of the nodes that sufficient decentralization has been achieved. *Delegates* are also responsible for oversight and maintaining the system. Unlike PoS, Delegated Proof-of-Stake *witnesses* do not compete intensely in adding the next block to the blockchain. As such it is an energy–saving system.

Smart contracts

A smart contract is a computer program built into a blockchain that contains a set of rules agreed to *a-prori* between parties such that it is automatically enforced once the predefined rules are met (Nelson, 2018). Put simply, a smart contract is a declaration of the form: *"transfer A to B if C occurs"*. The contract, once written into the blockchain, it cannot be altered and is extremely difficult to hack. It eliminates the need for a third trusted party, a central or enforcement authority, and thus reduces transaction costs. A smart contract is self-executing and self-enforcing permitting trusted agreements to be transacted among disparate and anonymous parties without recourse or the need for a central authority. The challenge in implementing smart contracts is whether or not they can be legally enforced for now, at least until legal and regulatory regimes come into existence.

Blockchain Categories

Blockchains can be grouped into two categories which are determined by the use to which the technology is applied. They are either private or public blockchains. They can further be subdivided into permissionless and permissioned blockchains. A public permissionless blockchain is one in which any interested party can participate. A private blockchain restricts participation to a group, usually an entity such as a government department or a public or private corporation. A private blockchain can be private and permissionless in which case participation is open to an entire group within a department or an entity. A private permissioned blockchain is one in which participation is ‘permitted’ to selected individuals or institutions. The main difference between permissionless and permissioned blockchains is that in the case of the latter, some form of authority, coordination, and oversight is required depending on the purpose to which the blockchain is put, while maintaining the basic elements and advantages of the blockchain (Nelson, 2018).

ADVANTAGES OF BLOCKCHAIN TECHNOLOGY

Blockchain technology through P2P association via computers acting as nodes has many advantages. Firstly, it eliminates the need for a central authority as a center of trust, resulting in faster transaction time and reduction of transaction costs such as fees. Secondly, in transacting business using blockchain, there is no need to create trust among the participants. The fact that each node has the same information as any other node eliminates the need for 'know-your-customer (KYC)'. Trust among participants is guaranteed using cryptography. Thirdly, the security of transactions is assured because the information contained in a blockchain is immutable. The hashed block is linked to all other blocks in the chain. It is almost impossible to retroactively change information contained in a block. An attempt to change a transaction in a block would necessitate a change to the hash of that block, requiring a large amount of time and computing power to accomplish the task. Fourthly, trust and confidence in the system is the hallmark of blockchain technology. Fifthly, the absence of a central authority creates an independent peer-to-

peer network that is self-regulating. Finally, increased transparency and immutability of records make blockchain technology ideal in the fight against corruption.

CHALLENGES AND RISKS

Decentralized ledger technologies including blockchain are at an early stage of evolution. While interest in blockchain technology is growing across many sectors, some limitations pose a challenge to its widespread adoption. Its inability to handle large volumes of transactions at high speed (scalability) is a major challenge. In bitcoin transactions, for example, it takes 10 minutes to add a block to the chain. A blockchain can only manage 7 transactions per second (tps). Compare this with 24000 tps which can be processed by Visa and 5000 tps by Twitter (Yli-Huumo et al., 2016). The inability of the blockchain to exchange data with other platforms, other blockchain types, and off-blockchain platforms (interoperability), is another challenge.

A large amount of computer processing power is required in order to implement the Proof-of-Work protocol. It is estimated that in 2018 bitcoin mining consumed 62.4 Terawatt-hours. This was the equivalent of the annual power consumption of Austria or 8 times the total annual electricity consumption of Tanzania (7.4 Twh). This brings into question the sustainability of large-scale use of technology (EU Blockchain 2019).

Honesty to be exhibited by nodes is the hallmark of a blockchain mechanism. However, the possibility of the existence of dishonest participants is always there. If such attacker nodes can muster at least 51% of participation, the blockchain system is vulnerable to what is referred to as a 51% attack.

Another disadvantage in the application of blockchain technology is inherent in the anonymity of participants. In the case of cryptocurrency exchanges, the system has attracted all sorts of undesirable activities such as fraud, tax evasion, money laundering, drug smuggling, racketeering, kidnapping, blackmailing, and funding of terrorist activities (Houbern & Snyers, 2018).

APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Blockchain is a nascent technology. As such, its use is being experimented in many sectors, with each new use adding more knowledge to the subject. Applications of blockchain are classified below into financial and non-financial applications. Financial applications include cryptocurrencies, and blockchain use in the banking sector, including central/reserve banks and the insurance industry.

Blockchain technology has led to the emergence of secure, reliable, and consensus-based cryptographic payment systems known as cryptocurrencies. The open source-code, permission-less blockchain description by Nakamoto (2008) of the bitcoin, has spurred on the creation of numerous cryptocurrencies such as Etherium, by Vitalik Buterin (Buterin, 2014), Ripple and others. By 20 November 2020, this development had led to the creation of 3789 cryptocurrencies with a market capitalization of US$ 524.12 billion (CoinMarketCap, 2010). Facebook initially conceived the *Libra*, a possible new global digital currency based on blockchain technology (Libra, 2019a; Libra, 2019b). Faced with possible regulatory negative feedback (Bernal, 2019; Bain & Weinstein, 2019; Hern, 2019), Facebook has come up with a new *Libra* (Libra, 2020), reduced in scope and scale (Dale, 2020).

Cryptocurrencies were initially viewed with suspicion and were almost ignored by banks. In some cases, these currencies have been variously described as a rat poison, an aberration, and ingenious

delusion (Helms, 2018). Many countries perceive cryptocurrencies as a threat to fiat currencies and their monetary systems. Cryptocurrencies are illegal in Algeria, Egypt, Bolivia, Thailand, Bangladesh, and in many other countries, while some countries, such as the USA, UK, Australia, Germany, Switzerland, and Malta have legalized them for use variously as foreign currency, a unit of account, an asset and as property (US Congress, 2018a; Ali *et al.,* 2014; Blumenfield et.al., 2018; Aberdeen, 2018; CRW, 2019; Finder, 2019).

The banking sector is cautiously moving towards the exploitation of blockchain technology's potential strengths, including near real-time transactions execution (Shah & Jani, 2018). Areas of interest in the application of blockchain technology to banking and finance include onboarding transactions among banks including a possible centralized Know-Your-Customer (KYC) information, exporters, importers, and corresponding banks on a blockchain system, derivatives, corporate bonds, smart contracts, syndicated loans, and some back-office operations, cross-border transactions (JPMorgan, 2019; Huillet, 2019; Nextweb, 2019; WEF, 2016).

Several Central or Reserve Banks across the world have started to embrace blockchain technology (News BTC, 2018; Pollock, 2019; Watson, 2019; Duros, 2019). They are exploring the possibility of issuing blockchain-based national digital currencies (Central Bank Digital Currency-CBDC) to be used to manage ownership and transfer of payments (Manchini-Griffoli *et al.,* 2018; Mbogo, 2019). The G20 Countries have recognized the need to establish a regulatory framework for crypto assets (Wall, 2018). The IMF has also advised Central Banks to consider cryptocurrencies (Lagarde, 2018; Niru, 2018).

While China has banned trading in cryptocurrencies, it has embraced the underlying technology to be one of the tools for scientific and industrial development (CAICT, 2018). China now leads the world in the development and application of blockchain technology (Wood, 2019). The People's Bank of China (PBOC) has been developing a digital currency that would be backed by the Renminbi, RMB (Das, 2016; Bloomberg, 2019). Trials of its digital Renminbi have started (PRC, 2020). The aim is to ultimately phase out the paper currency.

In Africa, Central Banks and Capital Market Authorities are taking a more cautious approach in embracing the blockchain technology. In many of these countries, participants in the cryptocurrency business are warned of the downside and risky nature of the trade (Ngugi, 2019; SARB, 2014; CBoK, 2015). Exceptions in this regard include Senegal and Tunisia, which have already launched national digital currencies (O'Neal, 2018).

In the insurance industry, if claims could be put into an immutable ledger, and insurance and reinsurance policies executed by smart contracts, stability, security, speed would be assured, leading to a reduction in premiums and trust among the insured, insurers, regulators, and governments (Cummings, 2018; CBinsights, 2019).

Non-financial applications of blockchain technology are being explored in ownership of land and property titles being held immutably. Blockchain technology is also now being exploited in tracing the agricultural supply chains from provenance to end–use. It enables traceability of products from cultivation, treatment, harvesting, transportation, storage, and sale (Gardner, 2018; Gerald, 2019; Foodtank, 2019). Ethiopia has established a blockchain-based tracking system for its world-famous Ethiopian coffee supply chain from the farmer to the user.

Blockchain technology can be used to keep patients' health, illness, and treatment records immutable. It can also transform the pharmaceutical industry through recording the drugs supply chain from production to hospitals and drug stores, and in reducing incidences of counterfeit drugs.

Blockchain technology is now being used to establish the source and authenticity of minerals. Such information can be used to inform the buyer of the final product about the mine from which the raw material was sourced and where it was processed (De Beers, 2018; Partz, 2019; Lewis, 2018; Nicola, 2019; Khatri, 2018). The buyer and the responsible authorities can verify whether or not: the mineral comes from a country under sanctions; whether the raw mineral has been mined using standard procedures.

Other uses and possible uses of blockchain technology include: digitization, storage, and verification of contracts and other security and non-security documents as is required in notary services; tracing the origin of such materials in the automobile industry to make sure that it is sourced from 'authorized' suppliers; tracing of mileage performance of trucks over a journey; trade in renewable energy through micro-grids (Nsikak, 2018); facilitation of trade through tamper–proof recording of transactions involving the supply chain from production, transportation, shipping, import clearance, distribution and sale (Norberg, 2019); reduction of the risk of cyber-attacks ;Blockchain and Internet-of Things-IoT (Miraz, 2019); and in elections by making a vote a block in a blockchain, thus eliminating tampering and rigging (Hamilton, 2018; GoK, 2019).

The development and wide–scale application of any technology are facilitated by standardization. The International Standards Organization (ISO), through its Technical Committee TC 307, is at various stages in the development of standards and guidelines for the blockchain technology (ISO, 2019a; ISO, 2019b). The ISO plans to roll out the first blockchain and distributed ledger standards, ISO/TC 307, by the year 2021 (Anjum, et al., 2017; Morris, 2018). The advancement of knowledge in the blockchain field, facilitated by standardization, should ultimately depend on education and research.

EDUCATION AND RESEARCH IN BLOCKCHAIN TECHNOLOGY AND APPLICATIONS

Blockchain technology can be used to store and permanently secure records of continuous assessments, examination results, academic qualifications, awards, accreditation, licensing, and intellectual property. With the advent of blockchain technology the end of paper qualifications could be near. Few universities in Africa are involved in education, training, and research in what has been billed as the most important and transformative technology since the invention of the Internet. The nascent nature of these technologies is such that universities in Africa are well placed to compete in the contribution of new ideas, the introduction of new applications, and involvement in research, development, training, consultancy, and partnership with business startups. After all, the foregoing constitutes the core mission of any university.

There is a wide scope for rigorous research on the ramification of blockchain technology application on the economy. In this regard, multidisciplinary research may be required to evaluate the societal impacts of blockchain systems application. Blockchain technology application is likely to lead to unemployment. Who will be impacted? What mitigation measures could be taken to lessen the impact of youth unemployment? How can blockchain technology be applied to expand financial inclusion in developing economies? Africa is a continent that depends largely on agriculture. How can countries leverage blockchain technology in the management of agriculture? How could blockchain be applied in tracing agricultural inputs such as seeds, fertilizers, and

pesticides? In what manner will blockchain application in tracing produce to market be beneficial to farmers? How will existing business models including the creation of value, management, and organization be disrupted by blockchain-based systems? What are the challenges and opportunities for research in the health and allied sectors? What are the ramifications of national CBDC to international currency exchange and trade?

The blockchain poses many challenges while at the same time creating opportunities for new perspectives, applications, and science research (theoretical and applied), computing, mathematics, cryptography, decision theory, regulation, trade, finance, business and innovation, agriculture, land and property ownership, and other fields.

CONCLUSION

Much of the literature on blockchain technology has been about its use in bitcoin and cryptocurrencies in general. The potential applications of blockchain go much further than virtual currencies. Disruptive as blockchain technology may be, it is also transformative in the sense that it is heralding new models in finance, business, management, and other applications.

Governments and Central Banks are considering how to regulate cryptocurrencies. While there is a need to regulate cryptocurrencies, legislation and regulation should arise from an informed perspective and should not be at the expense of the underlying technology. Positive aspects should be accommodated while mitigating against potential negative impacts of the technology. Laws and regulations should recognize smart contracts and digital signatures that underpin such contracts. Disputes will necessarily arise in the application of smart contracts across many jurisdictions. There will be a need to establish settlement mechanisms and enforcement challenges arising therefrom.

Central Banks are at various stages in the development of local digital currencies. In this regard, Central Banks need multi-agency involvement in the creation of such digital currencies, guided by national policies. African countries are advised to learn from the experience of Mauritius, Kenya (GOK, 2019), Uganda (Masereka, 2019), Rwanda (Butera, 2019), and South Africa (RSA, 2019; SARB, 2019) as they develop policy frameworks for the application and use of blockchain and other 4IR technologies.

While much work is currently being undertaken on the advances and utilization of this nascent technology, there is a paucity of scholarly output, particularly from African centers of learning there is a wide scope for universities, especially in Africa, to carry out cutting-edge research into blockchain and related 4IR technologies and their utilization.

Over the last decade, efforts have been made to address gender disparity in science, technology, engineering, and innovation, globally and particularly in Africa. In the case of 378 crypto and blockchain technology firms surveyed, women represented only 8.5 percent as founders or co-founders (Partz 2020). The development of an emerging technology of the type of blockchain should, ideally, present an opportunity to address the gender imbalance in favor of women. Policies for the development and exploitation of 4IR technologies need to factor in the promotion of women in Science, Technology, Engineering, and Mathematics (STEM), and innovation.

REFERENCES

Aberdeen (2018). Malta Becomes First Country to Regulate Cryptocurrency. *Aberdeen*, 28 September 2018.

Ali, R., Barrdear, J, Clews, R., & Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, 54(3), 262-275

Anjum, A., Sporny, M. & Sill, A. (2017). Blockchain Standards for Compliance and Trust. *IEEE Cloud Computing*, (4)84-90. July 2017.

Anoop, M.S. (2018). Elliptic Curve Cryptography. *InfoSec Writers,* April 2018.

Bain, B. & Weinstein, A. (2019). Facebook Says Libra won't launch until Regulators Satisfied. *Bloomberg*, 15 July 2019.

Baliga, A. (2017). Understanding Blockchain Consensus Models. Persistent Systems Ltd. April 2017.

Bayer, D; Harber, S. & Stornetta, W. (1992). Improving the Efficiency and Reliability of Digital Time-Stamping, *Sequences*, (2) 329-334.

Bernal, N. (2019). France to block the development of Facebook's digital currency Libra. *The Telegraph,* 12 September 2019.

Bitcoin Core Developer Reference. (n. d.).

Bloomberg (2019). China's PBOC Says Its Own Cryptocurrency Is 'Close' to Release. *Bloomberg News*, 12 August 2019.

Blumenfield, M., Horn, M., Ames, K., Riana, N., Munoz, C., & Paulsen, M. (2018). Carving up crypto: Regulators begin to find their footing. Regulatory brief. A publication of PwC's financial services regulatory practice. PwC, 2018

Butera, S. (2019). Rwandan Central Bank Studying Ways of Issuing Digital Currency. *BNN Bloomberg News*, 22 August 2019.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper

CAICT (2018). Blockchain White Paper (2018). China Academy of Information and Communication Technology and Trusted Blockchain Initiatives, December 2018

CBinsights (2019). How Blockchain Could Disrupt Insurance. *CB Research*, 10 January 2019.

CBoK (2015). Caution to the Public on Virtual Currencies such as Bitcoin. Central Bank of Kenya, December 2015.

CoinMarketCap (2020). Cryptocurrency market cap rankings, charts, and more. *Cryptocurrency Market Capitalizations (CoinMarketCap),* 20 November, 2020.

CRW (2019): France Adopts New Crypto Regulations. *Company Registrations Worldwide (CWR),* 24 May 2019.

Cummings, R. (2018). How Blockchain is Disrupting the Insurance Industry. Financial Innovation, CIO, 28 August 2018.

Dale, B. (2020). The Libra Association is Pulling Back from its Original Vision of a Global Digital Currency Backed by a Basket of National Currencies in a Bid to Appease Global Regulators. *Coindesk,* 16 April 2020.

Das, S. (2016): China's Central Bank Will Look to Issue its Own Digital Currency "as Soon as Possible", *CCN*, 21 January 2016.

De Beers (2018). De Beers Group Successfully Tracks First Diamonds from Mine to Retail on Industry Blockchain. *DBCompany News,* 10 May 2018

Decent (2019). Blockchain Architecture. *Pluralsight*, 10 January 2019.

Drescher, D. (2017). Blockchain Basics: A non-technical introduction in 25 steps. Springer Science + Business Media, New York 2017.

Duros, S. (2018). Cryptocurrency and Blockchain: Background and Regulatory Approaches. *Wisconsin Policy Project*, 1(2), September 2018. Wisconsin Legislative Reference Bureau. Madison, Wisconsin, USA.

EU Blockchain (2019). Scalability Interoperability and Sustainability of Blockchains. A Thematic Report prepared by the European Union Blockchain Observatory and Forum, 6 March 2019.

Finder (2019). Global Crypto Regulations-2019. Index of cryptocurrency regulations by country (updated 28 November 2018).

Foodtank (2019). The World Food Program: Fighting Hunger with Blockchain, Foodtank, January 2019.

Fortney, L. (2019). Blockchain, Explained. *Investopedia,* 21 May 2019.

Gardner, B. (2018). Merkle Tree Hashing: How Blockchain Verification Works. *CoinCentral*. 3 September 2018.

Gerald, S. (2019). E-Agriculture in Action: BLOCKCHAIN for Agriculture Opportunities and Challenges. Food and Agriculture Organization of the United Nations and the International Telecommunications Union, Bangkok, Thailand, 2019.

GOK (2019). Emerging Digital Technologies for Kenya: Exploration and Analysis. Report of the Taskforce on Blockchain and Artificial Intelligence. Ministry of Information, Communications, and Technology. Government of Kenya, 2019.

Hamilton, D. (2018). Kenya Elections Agency to Adopt Blockchain for Vote Transparency. Bloomberg, 20 August 2018.

Harber, S., & Scott, W. (1991). How to Time-Stamp a Digital Document, *Journal of Cryptology*, 3, (2)99-111.

Helms, K. (2018). Warren Buffett calls Bitcoin a Delusion-But an Ingenious One. *Bitcoin News*, 28 May 2018.

Hern, A. (2019). Libra: US Congress asks Facebook to pause development. *The Guardian,* 3 July 2019.

Houbern, R., & Snyers, A. (2018). Cryptocurrencies and Blockchain: Legal context and implications for financial crime, money laundering, and tax evasion. European Parliament, EU Directorate-General for Internal Policies, PE 619.024, July 2018.

Huillet, M. (2019). Santander Issues $20 Million End-to-End Blockchain Bond on Etherium. *Cointelegraph,* 12 September 2019.

IHODL (2018). What is Blockchain in Layman's Terms. *IHODL,* 4 September 2018.

ISO (2019a). Blockchain and distributed ledger technologies. International Organization for Standardization, ISO/TC 307.

ISO (2019b). ISO/TC 307 Blockchain and distributed ledger technologies, International Organization for Standardization. Participation. 2019.

JPMorgan (2019). Large Number of Banks to Join Live Application of Blockchain Technology.

Khatri, Y. (2018). Rwanda Starts Tracking Conflict Metal Tantalum with Blockchain. *Coindesk,* 17 October 2018.

Kwatra, K. (2017). Blockchain: The Byzantine Generals Problem. *Wolverine Blockchain,* 23 November 2017.

Lagarde, C. (2018). Winds of Change: The Case for New Digital Currency. International Monetary Fund. Singapore Fintech Festival, 14 November 2018.

Lamport, L., Shostak, R., & Pease, M. (1982). Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems,* 4 (3) 3 382-401.

Lewis, B. (2018). Blockchain to track Congo's cobalt from mine to mobile. *Reuters,* 2 February 2018.

Libra (2019a). A White Paper from the Libra Association Members: An Introduction to Libra.

Libra, 2019b, "The Libra reserve", https://libra.org/en-US/about-currencyreserve/#the_reserve.

Libra (2020). Libra White Paper: Blockchain, Association, Reserve. White Paper v2.0 From the Libra Association Members.

Mancini-Griffoli, T., Martinez Peria, M. S., Agur, I., Ari, A., Kiff, J., Popescu, A., & Rochon, C. (2018). Casting Light on Central Bank Digital Currencies. IMF Staff Discussion Notes 18/08, International Monetary Fund.

Masereka, A. J. (2019). Details of the Fourth Industrial Revolution Task Force Launched by Museveni. *Business Focus,* 8 April 2019, Kampala, Uganda.

Massessi, D. (2018). Byzantine Fault Tolerance in a nutshell. *Coinmonks*, 6 October 2018.

Massessi, D. (2019). Blockchain Consensus and Fault Tolerance in a Nutshell, *Coinmonks,* 6 January 2019.

Mbogo, A. (2019). South African Reserve Bank to Conduct Central Bank Digital Currency Feasibility Study. *BlockchainTechnology*. BitcoinAfrica.IO, 31 May 2019.

Miraz, M. (2019). Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies. Research Paper No. 2019-13. The Chinese University of Hong Kong.

Morris, N. (2018). ISO blockchain Standards Planned for 2021. *Ledger Insights,* June 2021.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, October 2008.

Nelson, P. (2018). Primer on Blockchain; How to Assess the Relevance of Distributed Ledger Technology to International Development. USAID. 30 April 2018.

News BTC (2019). Bank of England Chief Economist Thinks Bitcoin Could Replace Cash. *News BTC,* 18 May 2019.

Nextweb (2019). Big Banks launching a Blockchain Trade Platform Powered by 'Bitcoin-like' token. *TNW Hard Fork*, 3 June 2019.

Nicola, S. (2019). Using Blockchain to Help Fight Conflict Minerals. *Bloomberg Businessweek,* 24 April 2019.

Niru, J. (2018). IMF's Lagarde Asks Central Banks to Consider Cryptocurrency. *The Kenya Wall Street*, 14 November 2018.

Norberg, H. 2019). Unblocking the Bottlenecks and Making the Global Supply Chain Transparent: How Blockchain Technology Can Update Global Trade. A joint Policy Paper from The School of Public Policy, University of Calgary and the Canadian Global Affairs Institute, April 2019.

Nsikak, J. (2018). Blockchain can Revolutionize the Energy Industry in Africa, World Economic Forum, 29 November 2018.

O'Neal, S. (2019). State-Issued Digital Currencies: Countries which Adopted, Rejected, or Researched the Concept. *Cointelegram,* 19 July 2019.

Partz, H. (2019). Russia's Ministry of Education Introduces System for Tracking Diamonds via Blockchain. *Cointelegram*, 30 January 2019.

Partz, H. (2020). LinkedIn Co-Founder Blue Outlines Risks of Blockchain Sexism: WEF. *Cointelegram,* 24 January 2020.

Pollock, D. (2019). BMW Opens Its Doors for Mobility. Open Blockchain Initiative's First European Colloquium, *Forbes*, 5 February 2019.

PRC (2020). Digital Currency Trials Are Underway. The State Council of the People's Republic of China, 21 April 2020.

Ray, S. (2017). Merkle Tree. *Hackernoon*, 15 December 2017.

Rosic, A. (2019). What is Blockchain Technology? A Step by Step Guide for Beginners. *Block Geeks*, 1 March 2019.

RSA (2018). Invitation to Nominate Candidates for Appointment to the Commission on the Fourth Industrial Revolution; Terms of Reference. Republic of South Africa Government Gazette No. 43078, 4 December 2018.

RSA (2019). President Appoints the Members of the Fourth Industrial Revolution. Republic of South Africa.

SARB (2014). Position Paper on Virtual Currencies. South African Reserve Bank, 2 December 2014.

SARB (2019). Request for Expression of Interest Publication Detail. South African Reserve Bank, 26 April 2019.

Schwab, K. (2016). *The Fourth Industrial Revolution.* World Economic Forum.

Shah, T. & Jani, S. (2018). Applications of Blockchain Technology in Banking and Finance. Researchgate Technical Report No. 160617200028, February 2018.

Stolp, J. et al. (2019). Blockchain and Cryptocurrency in Africa: A comparative Summary of the reception and regulation of Blockchain and Cryptocurrency in Africa. Baker McKenzie, February 2019.

Tanul, C. (2018). The Kenya Blockchain Taskforce Concludes its Report. The Kenya Wall Street, 20 November 2018.

US Congress (2018a). Regulation of Cryptocurrency Around the World. The Law Library of Congress. Global Legal Research Center, June 2018.

US Congress (2018b). Regulation of Cyber Currencies in Selected Jurisdictions. Law Library of Congress. Global Legal Research Center, June 2018.

Vijayakumaran, S. (2017). An Introduction to Bitcoin. Abstract Lecture Notes on Bitcoin. Department of Electrical Engineering, Indian Institute of Technology Bombay, 4 October 2017.

Wall, J. (2018). G20 Leaders Agree to Establish Regulatory Framework For Crypto Assets. *Invest in Blockchain*, 4 December 2018.

Watson, E. (2019). Yahoo's Founder's Predictions for Bitcoin and Crypto are Bullish - He Forecasts a Great Impact on Finance's Future. *Oracle Times*, January 2019.

WEF (2016). The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services. The Future of Financial Services Series. *World Economic Forum*, August 2016.

Wood, A. (2018). China filed the most blockchain patents in 2017. *Cointelegraph*, 25 March 2018.

Wood, A. (2019). China Leading World in Blockchain Projects. *Cointelegraph.* 2 April 2019.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? – A Systematic Review. *PLoS ONE*. 11(10): e0163477. Doi:10.1317/ journal. pone.0163477.