DISTRIBUTED LEDGER TECHNOLOGY: SECURING THE ONLINE TRANSACTION ENVIRONMENT

APENE, Oghenevovwero Zion.
Department of Mathematical Science, Nasarawa State University, Keffi, Nasarawa State.
leazion247@gmail.com

IGE, Adeola A.
Department of Mathematical Science, Nasarawa State University, Keffi, Nasarawa State.
wealthyade@yahoo.com

HAMPO, Johnpal A.C.
Department of Computer Science, Federal University of Technology, Owerri, Imo State.
hampojohnpaul@gmail.com

OGEH, Clement Omamode
Department of Mathematics and Computer Science, Michael and Cecilia Ibru University, Agbarha-Otor, Ughelli, Delta State.
clementogeh@mciu.edu.ng

Abstract - Certificate Authority (CA) has played a major role in our modern digital economy. Most businesses using the internet rely on trusted third party. It can be a mobile banking App platform telling us that transaction is secured; it can be a mobile telecommunication service provider telling us that our calls, text has been delivered to intended party or a social media platform such as WhatsApp saying our chats and posts are end to end encrypted. It can also be Facebook telling us that post regarding life events can be seen only by those we want to see it; these third party can also be encrypted. With distributed ledger technology (also known as blockchain technology), we can have a better feel of the internet and participant in block can check and verify every transaction since the blockchain offer a more transparent environment. This paper focused on few strategic applications of Blockchain technology as reviewed by other authors. The study answered the following questions i. How does the blockchain technology work? ii. Where can blockchain technology be applied? and iii. What are the benefits of blockchain technology?

Keywords: Distributed Ledger, Blockchain, Bitcoin, Smart Contract, Smart Property, IoT, Trust, Privacy, Artificial Intelligence

I. INTRODUCTION

Blockchain is defined as “A distributed tamperproof database that secures all records that are added to it, wherever they exist. Each record contains a timestamp and secure links to the previous record” [1]. Blockchain technology has the potential to reduce the role of one of the most important economic and regulatory actors in our society’- the middleman. By allowing people to transfer a unique piece of digital property or data to others, in a safe, secure, and immutable way, the technology can create: digital currencies that are not backed by any governmental body; self-enforcing digital contracts (called *smart contracts*), whose execution does not require any human intervention; decentralized marketplaces that aim to operate free from the reach of regulation; decentralized communications platforms that will be increasingly hard to wiretap; and Internet-enabled assets that can be controlled just like digital property (called *smart property*).

Blockchain technology solves the problem of third party breach. It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction, past and present, involving digital assets can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two important characteristics of blockchain technology. The block comprises two important elements, the block and transactions, the transactions which are the actions initiated by participant belonging to a particular blockchain system while the block keeps track of these transactions and ensure that they are correct and are not compromised.

Storage in a blockchain structure

Fundamentally, blockchain is just a new way of storing and sharing information but it is different compared to the traditional method of storing information which is of relevance to the analysis of the applicable privacy rules. With blockchain, information is stored in a series of "information blocks” that are sequentially linked in a chain.

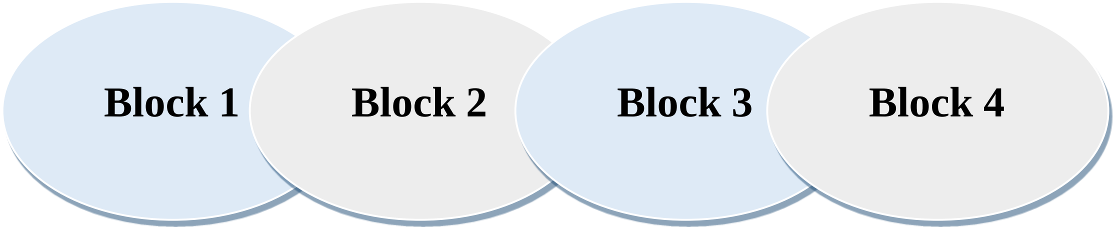

Figure 1: Blockchain Information System

“Generally, the analogy of a ledger is used to describe blockchain technology. With the blockchain as ledger, Block 1 would be the first page of that ledger. Every sequential block contains a hash (a far shorter, seemingly random sequence of letters and numbers) of the previous block. As a result, each block in the chain can be traced back to the original block. As each new page in the "ledger" contains a summary of sorts of the previous page or pages, the size of the ledger pages will increase over time. Thus, the idea of blockchain is that previous blocks of the blockchain cannot be altered or deleted undetected, because that would mean that each block thereafter would have to be regenerated. This *append-only* mechanism facilitates a maximum of insight in changes made to the blockchain. The effectuated *transparency and verifiability* help to prevent unauthorized changes.”

II. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed database for transaction processing. Although most current blockchains operate financial transactions, this is not necessarily the case; in the most generic case, transactions could be viewed simply as atomic changes to the system state. For example, a blockchain may be used to timestamp documents and secure them from alterations [2].

All transactions in a blockchain are stored onto a single ledger. As transactions are ordered by time, the present state of the system (in the case of a financial blockchain, the collection of all users’ balances) is uniquely determined by the ledger. Storing all transaction history has other benefits such as increased regulatory compliance and the ability to determine the state of the system at any specified moment of time by “replaying” corresponding transactions.

Blockchain is a database of information distributed over a network of computers rather than located on a single or multiple servers [3].

Generally, transaction processing with blockchain technology satisfies the following properties:

- **Transactions should conform to the present state of the system:** e.g., in the case of financial transactions, if Alice’s balance is $1,000, she cannot pay Bob $10,000.
- **Transactions should be authorized:** That is, only Alice should have an access to perform transactions using her name or authorized key or identity.

- **Transactions should be unmodifiable:** once transaction has entered the ledger, it should be impossible to modify its information (e.g., if there is a transaction in which Alice pays Bob $10, a perpetrator should not have the ability to change the sum of payment or its sender, or its recipient).
- **Transactions should be final:** once transaction is recorded in the ledger, it should be impossible to delete it, which would effectively reverse the transaction.
- **Censorship resistance:** if a transaction conforms to a ledger protocol, it should be eventually added to the ledger.

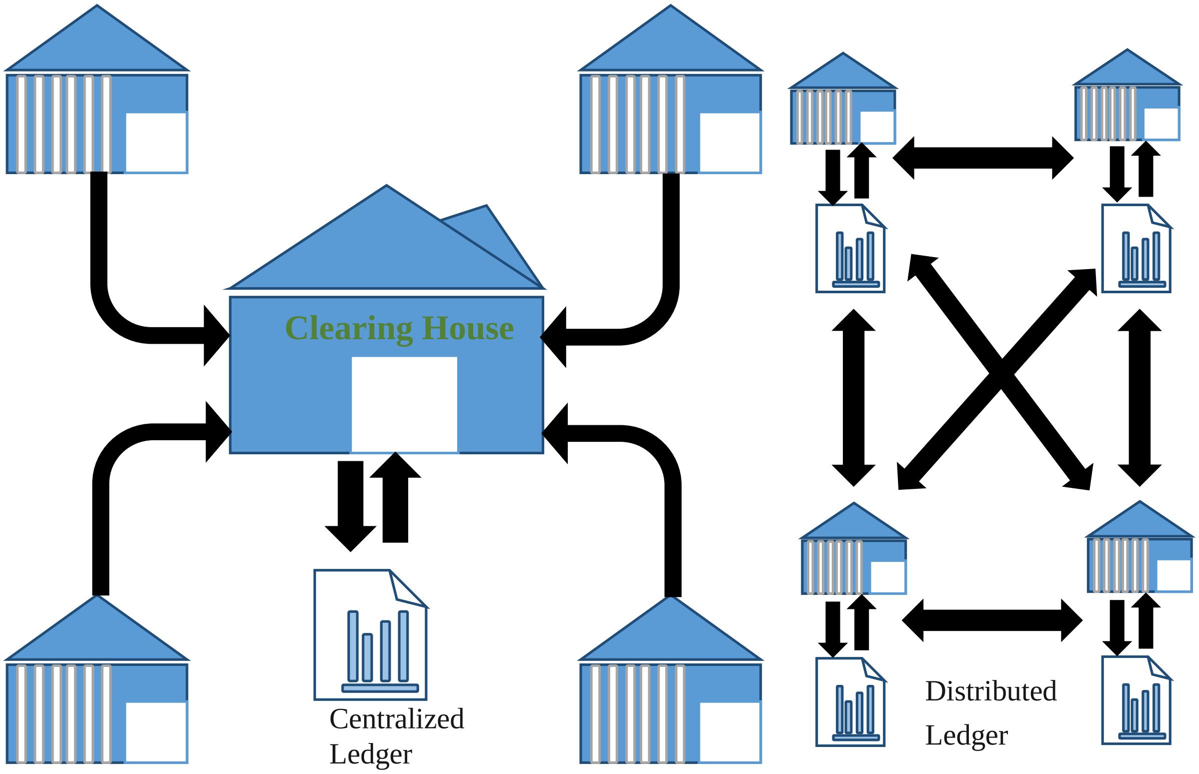

Figure 2: Introduction of the Blockchain Technology (Financial Times) adapted from [3].

A Blockchain is a replicated, shared/distributed ledger of transactions or asset holdings which enables “collective bookkeeping”

- It provides provenance, immutability and finality for the transfer of value within a business network.

- It enables value exchange in real time, reducing costs and errors.

• Based on a network consensus approach, whereby trust between the parties involved in a transaction is provided by cryptography (i.e., mathematics)

- This prevents “double spending” and protects the system from hacking, fraud, etc.

- Cryptography replaces the need for third parties/intermediaries which are not required to verify or clear transactions [4].

Blockchain can be classified into

I. Public or private, meaning they can be open to everyone or restricted to a defined group of users (e.g., institutions)

II. Permissioned or permissionless, meaning that either anyone can offer their services to add blocks to the chain or only a restricted group of users can do so.

III. EMPIRICAL REVIEW

[5], in her study of Privacy, Security and Blockchain suggested that when designing blockchain systems, the applicable privacy rules should be considered, as blockchain concerns the storage and exchange of data on a large scale, which may also include personal data. And that parties considering applying blockchain technologies in their transactions should also consider the privacy implications. If the privacy rules are applicable, it may be advisable to perform a data protection impact assessment (or to let one be performed) at an early stage and as such the relevant privacy aspects are mapped out, which should be taken into consideration with the further detailing of the blockchain application.

[4] Studied Unlocking the Real Benefits of Blockchain using sweet spot approach, and posited that Blockchain Technology can provide following key benefits if properly implemented.

- Mathematics used to enable trust between parties
- Secure yet shared view
- Full provenance and immutability
- Provision of comprehensive, rich information
- Automated verification/reconciliation
- Self-enforcing contract capability

[6] studied IoT and Blockchain and identified that blockchain Technology is the missing link for IoT devices since it will reduce cost, accelerate transactions and build trust. It also suggested that

when blockchain is deployed in IoT devices, it will eliminate single point of failure, thereby creating a better resilient ecosystem for IoT devices to interoperate. [1] studied Blockchain application in HealthCare, in their study they suggested that blockchain technology can help in great deal in the health sector in the following ways:

1. **Creating secured and trusted care records:** Securing healthcare records created by healthcare professionals and patients into an electronic chain of events, while preserving the inherent provenance and integrity of those records
2. **Linking identities:** Supporting strong identity proofing by preserving an immutable record of the declared identities of both patients and healthcare professionals.
3. **Recording patient consent:** Empowering patients through the recording of consent decisions and patient directives within the secured healthcare record

The study also posited that to protect the privacy of each user, healthcare organizations can also use a number of solutions such as tokenization, pseudonymization or masking technologies. The study concludes that, to be effective, a blockchain must be additive to the healthcare ecosystem; users should not view it as a “rip and replace” technology that invalidates or minimizes existing technology investments. Furthermore, despite the hype surrounding blockchain technology, it is not a cure-all for what ails the healthcare ecosystem but rather a tool in the healthcare toolbox, one that may face some of the same challenges current service models do. [7] in the Handbook of digital currency, examined Blockchain Electronic Vote, he found out that although there are existing voting systems, there are design flaws, lack of open source and have verifiability problem; these underlying problems has created trust issues between voters and election organizers, hence the need for an improved system. The study proposed that with the adoption of blockchain technology although might not totally eradicate all the problems electronic voting, but it will provide an improved system with following key benefits: Free, open-source peer-reviewed software, Ubiquitous, Secure, Protecting the secrecy of the ballots. Allowing free, independent audits of the results, minimizing the trust level required from the organizers. This also agrees with the study with [8] that blockchain provides a technology framework for a transparent recordkeeping where all transactions are transparent. Although digital voting has been in practice in most places, the issues with accountability and auditing makes it worrisome, with the potential of blockchain, these issues can be mitigated. The study also argued that although the Blockchain –based election system promises to be good, from the study and responses from most people interviewed, is the adoption and acceptability by most people, since people always stick to their own way doing things.

IV. APPLICATIONS OF BLOCKCHAIN: PRESENT AND FUTURE

Digital Identity

The uniqueness and security of blockchain enables its use for identity. The blocks can contain the details of an individual and the rate of identity theft will be on the decrease. Blockchain technology in identification enable the users to controls who have they data and how they can use the data. Some blockchain companies that have employed it for identification are UniqueID Wallet, Identifi, 2Way.IO and other [11].

E-Voting

The traditional paper ballot system is a very popular method of choosing leaders in a democratic system of government. This traditional ballot system has so many problems ranging from all forms of rigging which includes ballot stuffing, falsification of results, voter intimidation, the inability to track one's vote, vote buying, time wastage on queue for voting and counting of votes etc.

Although, several counties have tried the electronic voting but there are issues of security of data on a central server which can be solved by the Distributed Ledger Technology (DLT) due to its distributed and immutable nature. The decentralized and immutable nature of the Distributed Ledger Technology (DLT) enables voters to track their votes and even change their votes before a specific deadline there by making the entire process transparent.

Electronic voting (e-voting) of late has been the trending technology in democratic nations instead of manual and paper ballot or voting. However, some security issues are setback to it and the voting transaction can be tempered even though it is a real time system. To this effect, Follow My Vote platform uses blockchain technology in combination with elliptic curve cryptography to provide a secure and transparent online voting solution. Notably, NASDAQ and the Republic of Estonia in 2016 announced that Estonia's e-Residency platform will be facilitating a blockchain-based e-voting service to allow shareholders of companies listed on NASDAQ's Tallinn Stock Exchange to vote in shareholder meetings. NASDAQ's Tallinn Stock Exchange is Estonia's only regulated securities market.

Finance

The first application of the blockchain technology was Bitcoin, a digital currency which was based on a protocol that allows the users of the network to perform transactions with virtual money that exist only in their computers in a fast, and secure way.

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system [8].

A blockchain is a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. A block is the 'current' part of a blockchain which records some or all of the recent transactions, and once completed goes into the blockchain as permanent database which cannot be easily altered. Each time a block gets completed, a new block is generated. There is a countless number of such blocks in the blockchain. The blocks are linked to each other (like a chain) in proper linear, chronological order with every block containing a hash of the previous block. The blockchain is seen as the main technological innovation of Bitcoin, since it stands as proof of all the transactions on the network. Each node (computer connected to the Bitcoin network using a client that performs the task validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the Bitcoin network. The blockchain has complete information about the addresses and their balances right from the genesis block to the most recently completed block. To use conventional banking as an analogy, the blockchain is like a full history of banking transactions. Bitcoin transactions are entered chronologically in a blockchain just the way bank transactions are. Blocks, meanwhile, are like individual bank statements which Blockchain is kept up to date with the help of cryptography and copious computing power, provided by a global network of tens of thousands of computers. Openness in the chain helps the system remain secure: the blockchain is public so every participant can check and verify whether a transfer comes from the rightful owner.

Characteristics of Bitcoin Transactions

Transactions in Bitcoin **–** Bitcoin can be considered as chain of digital signature. Owner 1 transfer coin to owner 2 by digitally signing a hash of the previous transaction and the public key of owner

2, he then adds these to the end of the coin; here a payee can verify the chain of ownership. Bitcoin transactions can be verified without parties, transactions are publicly announced, and there is also a need for a system for participants to agree on a single history of the order in which they received.

Timestamp servers – The essence of timestamp server in bitcoin is to ensure the valid ordering of transactions. A time stamp server works similarly as in case of newspaper or Usenet, this is done by taking a hash of block of items to be time stamped and the hash can be published. Timestamping has been in existence, even before the advent of computers, information could be hashed and the hash published in newspaper. Timestamping of bitcoin allows one to anonymously timestamp information in a tamper proof in a faster way. Timestamp is created immediately a transaction is accepted to a blockchain and at various intervals.

Privacy of Bitcoin – The traditional banking system achieves a level of privacy by limiting access to the information to the parties involved in the transaction and a trusted third party. In bitcoin, all transactions are made possible by breaking the flow of information in another place: by keeping the public keys anonymous. This implies that the public can be aware a transaction is taking place, but to whom they do not know, ie they will know the information linking the transaction. This is only known to the two parties involved in the transaction.

Internet of Things (IoT)

Devices connected to the internet can use the blockchain as a persistent and highly-available storage solution, can use smart contracts to provide a global distributed computing capability, and can rely on the blockchain as a secure channel for receiving information about software and configuration updates and dynamically-delegated access control (including physical access control, for locking devices). Blockchain Technology can help IoT devices to transact in a more trusted environment since privacy and trust. With Blockchain Technology will allows IoT devices to be used in building solutions to help organizations improve operational efficiency, transform customer experience, and adopt new business models in a secure, private, and decentralized manner that will be of great value to all participating members.

Food Industry

Distributed Ledger Technology (DLT) is currently been applied to the tractability and transparency of food production and consumption in the food industry. According to [12] Walmart in collaboration with IBM is implementing the DTL to enable the total transparency of the food production and retail system. Hence a retailer or a consumer can trace easily the source of any food. The advantages of this food transparent system are so enormous. Some of which include the enhancement of food safety, availability of only fresh food in the open market, prevention of food wastage, avoidance of food fraud.

Cyber security

With the increase in the occurrence of cybercrimes, there is the need to secure data more efficiently in a network. The Distributed Ledger Technology (DLT) can be applied to solve the cybersecurity issues due to its immutability, the absence of human trust, decentralized and consensus traits. The consensus traits enable a democratic system for where nodes in the systems take a note to make a change in data.

Property Registration in the Real Estate Sector

In recent times, land fraud has gradually increased. With the Distributed Ledger Technology (DLT) the process of processing a land can be made transparent by making the land registration process open. Hence, investors can easily know genuine property that are in the real estate market.

Healthcare

The Distributed Ledger Technology (DLT) can be applied in managing diseases outbreak data and for the tracking of patients' health after they have been discharged from the hospital. [13] It can also be used to track a patient's medical record from various doctors.

Banking and Financial Institutions

The Distributed Ledger Technology (DLT) can be used in tracking financial transactions thereby checking fraud. It can also be used in making financial predictions as a result of the large amount of data and in fact, the large amount of distributed data in the Distributed Ledger Technology (DLT) is attracting interest from researchers in the field of big data analysis [14].

Entertainment Industry

The Distributed Ledger Technology (DLT) can be used in tracking and leasing of intellectual properties of artist such as song records, royalties, ownership of work and copy write issues in the entertainment Industry.

Transport and Tourism

The Distributed Ledger Technology (DLT) can be applied to car hiring and the optimization of hotel spaces.

V. FUTURE APPLICATION OF BLOCKCHAIN

Emerging Bank can use blockchain technology as general ledger. Blockchain technology has the ability to keep track of data like transactions, contracts, agreement and these can be also to verify, because of this potential, it can be used in asset management especially in the area of land certificate.

Blockchain Technology can make great impact in financial institutions since it can be used to keep track of details of any transaction or ownership of any asset like real estate management and intellectual property. It can also be used to automate contracts. Notable applications of Blockchain Technology may include:

- Smart contracts
- Physical asset registration (e.g. the issuance of Certificate of Occupancy)
- Trade execution and settlement
- Asset exchange
- Cash reserve management
- Supply chain management
- Stock exchange market
- Communication and social networks
- Insurance
- Education (bodies like WAEC, NECO, IELTS, TOEFL and so on)

VI. ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN

Artificial Intelligence is the science of making Machines think for themselves which when properly implemented can improve productivity and efficiency in many life endeavors. Machines can make better decisions by evaluating various parameters from its environment there by increasing the success chances in it application. Artificial Intelligence AI has been applied in mining the stock market, diagnosis of ailments in medicine, legal system, Engineering, Space Science etc. [10]

There are however areas where AI is deficient which can be improved by the integration of the Block Chain and Vice versa. The table below compares commentary features of Artificial Intelligence and Block Chain.

Table 1: The Complementary Features of Block Chain and Artificial Intelligence

	Artificial Intelligence	**Block chain**
1	Centric in Nature	Distributed
2	Dynamic	Deterministic
3	Probabilistic	Immutable
4	Volatile	There is data integrity and security
5	Data, Knowledge and Decision Centric	Attack resilient

Benefits of integrating block chain with Artificial Intelligence

1. **Enhanced Data Security:** Block Chain is a distributed transaction ledger, hence users' data are kept secured and immutable in various nodes of the network. However, the use of AI algorithms will further enhance the security of data by reporting or alerting user of fraudulent transactions or unauthorized access at the application level of one node.
2. **Collaborative Decision making:** With AI algorithms like the swarm algorithm where each unit in the swarm has a direct effect on the overall performance of the swarm, the decision making process can be enhanced with each node in the network performing optimally.
3. **Improved Data Integrity:** Users usually do not trust entirely decisions made by machines but with blockchain the integrity of data can be maintained by making sure that the decisions made by the machines are taken note of and stored in a distributed system where each node in the system keeps a copy of the data.

4. **Distributed intelligence:** Artificial intelligence algorithms can be applied in the consensus voting in the blockchain technology where the nodes in the blockchain perform different subtasks that have a common dataset.AI can also be applied in solving issues related to Security and Scheduling among the nodes in the underlying network.
5. **Increased Efficiency:** The integration of Artificial Intelligence and Blockchain enables the speedy and automatic validation of data, values and asset transfer among stakeholders. Other benefits of Blockchain and Artificial Intelligence as describe by Tshilidzi and Bo [9] are shown in the figure below

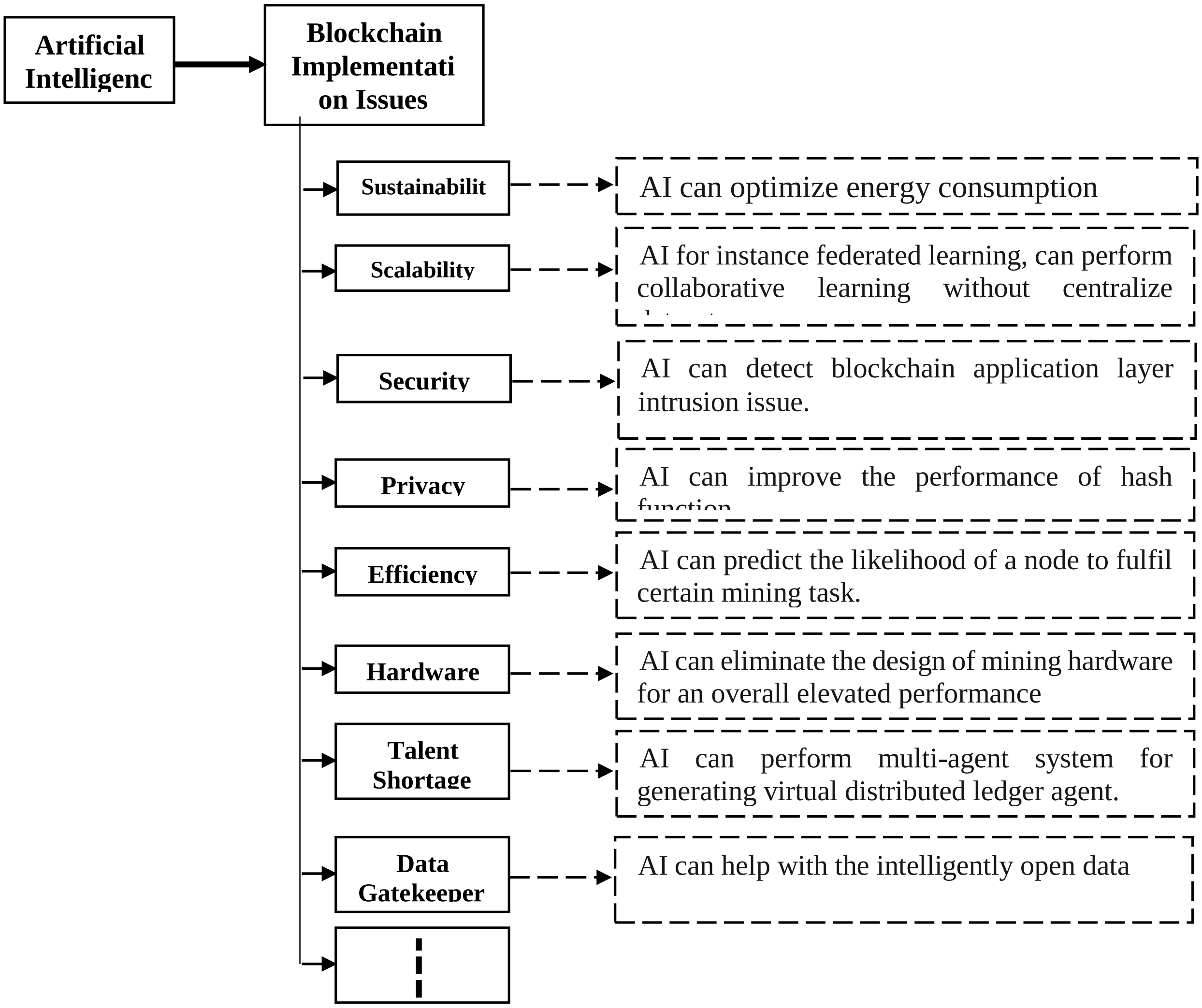
Artificial Intelligenc
Blockchain Implementati on Issues
Sustainabilit
AI can optimize energy consumption
Scalability
AI for instance federated learning, can perform collaborative learning without centralize
Security
AI can detect blockchain application layer intrusion issue.
Privacy
AI can improve the performance of hash function
Efficiency
AI can predict the likelihood of a node to fulfil certain mining task.
Hardware
AI can eliminate the design of mining hardware for an overall elevated performance
Talent Shortage
AI can perform multi-agent system for generating virtual distributed ledger agent.
Data Gatekeeper
AI can help with the intelligently open data

Figure 3: The Integration of the Blockchain and Artificial Intelligence. [9]

VII. CONCLUSION

Blockchain, although still at its preliminaries stages has attracted attention of many beyond the development space. Blockchain main applications is the cryptocurrency: bitcoin; which uses a peer-to-peer technology to carry out transaction with little or no intervention of trusted third party. With the growing adoption of digital technology for financial transactions, blockchain technology can offer a wide range of services to financial institutions which can help in good completive strategy against its competitors and increase efficiency. In the future blockchain can be adopted in land certificate administration, university certificate verification, assets management. It will also serve as a strong cryptographic technology behind many Apps ranging from mobile App to Desktop App. The future of blockchain is sure, just as the internet has made the world a global village.

REFERENCES

[1]. C. Brodersen, B Kalis, C Leong, E Mitchell, E Pupo, A. Truscott, L.L.P Accenture, "Blockchain: Securing a New Health Interoperability Experience" , 2016

[2]. G. BitFury and G. Jeff, "Public versus Private Blockchains: Permissioned Blockchains" White Paper, 2015

[3]. K. Kibum and K. Taewon, "Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology", OECD GLOBAL ANTI-CORRUPTION & INTEGRITY FORUM , 2017

[4]. ACI Worldwide, Inc. unlocking-benefits-of-blockchain available online at: https://www.aciworldwide.com/-/media/, 2016

[5]. Vandoorne https://www.vandoorne.com 2016/.../privacy-security-and-blockchain, 2016

[6]. Ahmed B. (2017): IoT and Blockchain Convergence: Benefits and Challenges: http://iot.ieee.org/newsletter accessed 21st, June, 2017

[7]. N. Pierre, "Blockchain Electronic Vote in Handbook of Digital Currency" Edited by David L.K.C, Academic Press, 2015

[8]. www.bitcoin.org

[9] Tshilidzi Marwala and Bo Xing, (2018), Blockchain and Artificial Intelligence University of Johannesburg, Auckland Park, Republic of South Africa, https://arxiv.org/ ftp/ arxiv/ papers/ 1802/ 1802.04451. pdf

[10] Salah K, Rehman M. H, Nizamuddin N. and Al-fuqaha, A, (2018), Block Chain and AI: Review and Open Research Challenges Institute of Electrical and Electronic Engineers (IEEE) Access. Accessed on 25th March, 2019 on www.Reseachgate.com. Digital Object Identifier 10.1109/ACCESS.2018.DOI

[11] https://gomedici.com/21-areas-of-blockchain-application-beyond-financial-services/. Accessed on: 31st March, 2019

[12] https://blockgeeks.com/guides/blockchain-applications-real-world/. Accessed On: 2nd April, 2019.

[13] https://coinswitch.co/news/20-blockchain-applications-across-industries-2018. Accessed On: 2nd April, 2019.

[14] http://www.dtoklab.com/big-data-and-blockchain/ Accessed On: 2nd April, 2019.