An in Depth Analysis of Blockchain Technology, and its Potential Industrial Applications

Yangsun Lee
Department of Computer Engineering,
Seokyeong University, 16-1 Jungneung-Dong, Sungbuk-Ku, Seoul 02713, Korea.
yslee@skuniv.ac.kr

Correspondence should be addressed to Yangsun Lee : yslee@skuniv.ac.kr.

Article Info
Journal of Machine and Comp uting (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303045
Received 18 April 2023; Revised from 28 July 2023; Accepted 26 August 2023.
Available online 05 October 2023.

Abstract – The emergence of blockchain technology represents a significant advancement in the field of computer science. Blockchain, an innovative technology that functions as a decentralized and publicly accessible record of all financial transactions, has significantly transformed the manner in which commercial activities are conducted. Companies and large-scale technology corporations have started substantial investments in the blockchain industry, a sector that experts forecast will exceed a valuation of $3 trillion during the next five-year period. The surge in its popularity may be ascribed to its robust security measures and comprehensive resolution for all issues pertaining to digital identity. The system in question is a decentralized digital ledger. A blockchain refers to an immutable and decentralized ledger composed of blocks, which function as collections of entries. The interconnection among these blocks is secured using encryption. The blockchain technology is captivating due to its inherent qualities, and it has significant potential in several domains owing to its desired attributes such as decentralization, transparency, and irreversibility. While blockchain technology is now most prominently associated with cryptocurrency, it has a diverse array of potential applications. This article aims to explore the many applications of blockchain in the domains of voting mechanisms, Internet of Things (IoT), supply chains, and identity management.

Keywords – Blockchain Technology, Distributed Ledger Technology, Decentralized Ledger, Voting Mechanism, IoT Management, Supply Chain Management, Identity Management.

I. INTRODUCTION

In recent years, the financial services industry has seen a significant amount of attention and capital allocation towards Distributed Ledger Technology (DLT). DLT, which is often referred to as blockchain technology or distributed database technology, is an alternative term used to describe this particular technological innovation. A ledger may be defined as a kind of database that maintains a record of transactions in a sequential order, with each entry being accompanied by a timestamp indicating the time of occurrence. When a bank client initiates the registration process for an online banking account, the financial transactions of such customer are systematically documented in a sequential manner. A number of prominent financial institutions have established research divisions to explore the potential of the technology, while many market entities have formed collaborations to establish standardized protocols. The user's text is too short to be rewritten academically. According to research conducted by the World Economic Forum in 2016 [1], an expenditure above $1.4 billion has been allocated towards the exploration and implementation of this technology within the financial services industry during the preceding three-year period.

Businesses often use several ledgers to effectively monitor financial transactions across diverse departments and activities. In order to facilitate internal reporting to management and external documentation in business reports, balance sheets, and income statements, it is essential to ensure the permanent reconciliation and consolidation of these distinct ledgers into a unified general ledger. Every company and organization have a ledger that is safeguarded using cryptographic measures. According to the illustration shown in **Fig 1**, it is evident that the individual vested with the responsibility and authorization to modify the ledger, namely the act of recording information, is the corporate accountant.

Blockchain technology grounded on the ideology of decentralized database, whereby data is replicated across several devices to achieve decentralization. The decentralized structure of blockchain renders it resistant to hacking, in contrast to businesses that use centralized databases, which expose themselves to potential security breaches. The concept of blockchain may be conceptualized as a distributed network of computer systems that functions on the foundation of the pre-existing

internet infrastructure. The layered architecture of a blockchain has three fundamental components: applications, the distributed ledger, and the peer-to-peer network. The network may be seen as including three tiers: the uppermost layer consists of apps, the middle layer encompasses a distributed ledger, and the lowest layer is constituted by a peer-to-peer network. The application software of the Blockchain may be located inside the network's "application layer." In order to safeguard their unutilized Bitcoins, individuals have the option to use Bitcoin wallet software, which is responsible for the creation and management of private and public keys. The application layer provides a user-friendly transaction tracking interface that is readily comprehensible to human users.

According to Tanwar [2], the inclusion of a Decentralized Ledger layer inside a blockchain architecture serves the purpose of ensuring the verification and maintenance of a reliable and unchangeable global ledger. In this context, financial transactions may be consolidated into groups and safeguarded by the use of cryptographic hashes. In a transaction, parties engage in the exchange of tokens, which are subject to a validation process prior to their acceptance. The process of mining transactions occurs when a novel block is generated and then added to the preexisting blockchain. The determination of the most labor-intensive blockchain construction and the establishment of consensus among all nodes about the genuine blockchain are facilitated by the implementation of a proof of work (PoW) algorithm inside the blockchain system. The Peer-to-Peer Network serves as the fundamental infrastructure for the blockchain architecture. In this context, several types of Nodes are responsible for executing distinct functions, while a multitude of messages are exchanged to ensure the seamless operation of the Distributed Ledger.

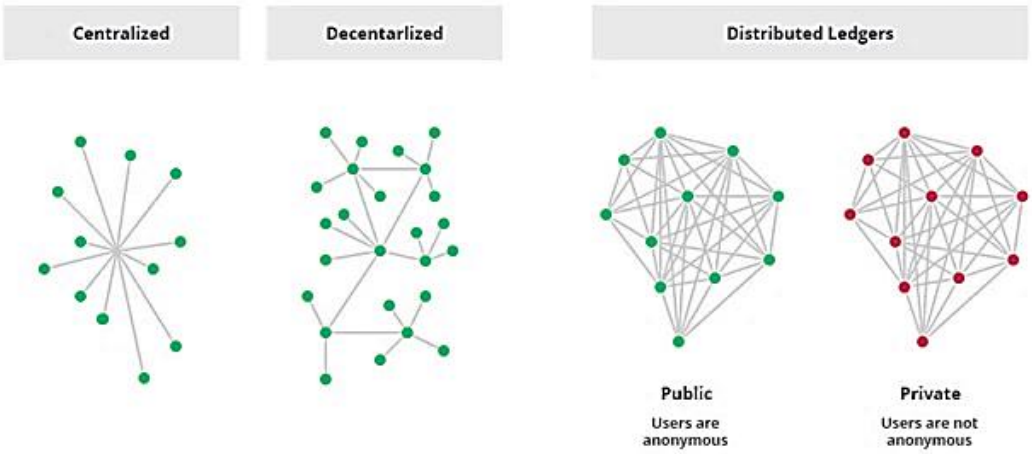

Fig 1. Centralized, Decentralized and Distributed Network Models

This article presents a comprehensive analysis of the many uses of blockchain technology, specifically focusing on its potential as a voting mechanism, IoT management solution, supply chain tool, and identity management system. The remainder of the article has been organized as follows: Section II presents the main discussion of the article, which includes blockchain applications as a voting mechanism, IoT management, supply chain management, and identity management. Section III concludes the paper and provides directions for future research.

II. APPLICATIONS OF BLOCKCHAIN

Voting Mechanism

ccording to Jafar, Aziz, and Shukur [3], the process of casting votes, whether via traditional paper-based methods or technologically advanced electronic systems, plays a pivotal role in fostering the development and progress of democratic societies. Traditional voting involves physically visiting a designated polling location, queuing in line, and personally submitting a ballot. A significant portion of the population abstains from voting due to factors such as physical absence from the polling location, skepticism over the efficacy of their vote, or lack of confidence in the electoral system. Electronic voting, often known as e-voting, presents a potential resolution to the aforementioned concerns. The use of electronic voting systems obviates the need for voters to physically visit designated polling locations and endure the inconvenience of queuing, therefore affording them the convenience of casting their votes from any geographical area around the world. There are many challenges associated with remote electronic voting. Strict security precautions are necessary due to the potential for hacking activities, the risk of large-scale manipulation, and the presence of coerced or influenced voting. Blockchain technology presents a viable solution to the aforementioned issues because to its inherent immutability features, transparency, and resistance to hacking, which effectively deter any attempts to manipulate the results.

Mukherjee, Majumdar, Kolya, and Nandi [4] developed a protocol for peer voting with the aim of preventing voter impersonation and enabling the identification and rectification of fraudulent activities, all while eliminating the need for external intervention. The protocol is founded upon the following fundamental concepts: One such approach is referred to as "distributed voting," whereby voters are provided with many ballots and the outcome is determined by calculating the median. This arrangement guarantees the preservation of privacy in the voting process. The responsibility of counting votes

is assigned to individual peers via the use of a homomorphic encryption algorithm, hence leading to the establishment of a distributed tally. By doing so, the involvement of a third party is eliminated, thereby guaranteeing that no peer has access to all of the results. Regarding the third issue, the use of cryptography for the purpose of verifying votes aids in the detection and elimination of fake ballots, so ensuring that only individuals of integrity have participated in the voting process. The process of verifying votes may be conducted in a transparent manner that respects the privacy of voters, making the involvement of other entities unnecessary. The voting process consists of five sequential phases in **Table 1**, necessitating the use of both off-chain and on-chain computations.

Table 1. Stages Involved in the Voting Process

Stages	Process	Brief description
Stage 1	Voting	During this phase, voters use client apps during the designated timeframe to generate and submit their votes on the blockchain platform.
Stage 2	2-Phase ballot verification	During this phase, each vote undergoes decryption and verification by peers who possess the Homographic Encryption Public Key (HEPK) necessary for encrypting the ballot.
Stage 3	The process of re-voting ballots encrypted using the public key of untrustworthy peers	A peer is faced with a decision between abstaining from replacement, resulting in the exclusion of the ballot labeled as "to be replaced" from the voting process, or opting to cast a new ballot. In the latter case, the peer may use another peer's HEPK to encrypt the ballot. Stage 3 is implemented in the event that a need arises to substitute the ballot.
Stage 4	Distributed Tally	During this phase, each participant with integrity calculates the votes and publicly discloses the outcome on the blockchain. The verification of each peer's tallies is facilitated by the use of homographic encryption characteristic inside the smart contract. In the event that an inaccurate count is identified, the associated peer will be accused of dishonesty, prompting a repetition of Stage 3 until all instances of dishonest tallies have been eliminated.
Stage 5	Final Aggregation	During this phase, the collective outcomes of the tally obtained from peers are consolidated via the use of a smart contract, ultimately leading to the publication of the final vote result on the blockchain.

The researchers conducted an evaluation of the protocol using Hyperledger Fabric and determined that it exhibited compatibility with voting problems characterized by low to medium levels of complexity. The classification of blockchains encompasses three separate categories, namely public, private, and consortium. Public blockchains are often regarded as being fully decentralized because to the absence of a central authority governing their consensus mechanism. Instead, the consensus is achieved via the competition among computing power and the dissemination of public information. Although the consensus technique has several benefits, its use in commercial settings is limited due to two primary reasons. Firstly, it incurs substantial energy wastage. Secondly, the efficiency of transaction validation is diminished as a result of competition for computer resources. The process of block production and transaction verification in this system relies on an uncontrollable network-wide decentralized verification mechanism, which does not adhere to commercial social regulations and has challenges in meeting business society norms.

Li, Li, Hou, Li, and Chen [5] established a consensus process known as Proof of Vote (POV), which relies on voting as its basis. The main objective of this study was to showcase the ability of POV to achieve outstanding performance in transaction verification with little latency. This might be advantageous in the context of consortium blockchains. The design of the consensus mechanism incorporates the concept of "proof of vote," which is reflected in **Fig 2** via the presence of two distinct sorts of votes. One vote supports the adoption of block manufacturing, and the other vote advocates for the retention of the butler staff. In order to cast a vote, it is necessary for every commissioner to provide their signature. A syndicate committee is established through the collaborative efforts of many firms with the aim of facilitating efficient sharing of data and information. To guarantee effective representation, each participating company appoints a commissioner to serve on the committee. A selection of butlers is designated to oversee and produce blocks, since it is deemed unwise to entrust complete management of the blockchain to any one organization. The selection of butlers is carried out by the commissioners, since it is within their jurisdiction to provide suggestions, cast ballots, and offer evaluations of potential applicants. In order to pursue a career as a butler, it is necessary to initially: 1. Aspire to pursue a career as a candidate for the position of a butler. 2. Assuming the role of a butler via the process of election.

The commissioners proceeded to use their voting rights in selecting the prospective candidates for the position of butlers. Commissioners, butlers, butler candidates, and users all use cryptography as a means of authentication. The individuals fulfilling the role of butlers within this consensus process are responsible for the generation of blocks at certain intervals. The first block, represent the genesis block, is created via the input of data by commissioners. Conversely, the final block, known as the consensus block, has details pertaining to the elections and the servers of the recently appointed butler nodes. The creation of each legitimate block occurs via a sequential process consisting of eight phases inside the round of agreement. The recently formed block is thereafter sent to all commissioners for their approval. In order for a block to be deemed legal,

it is necessary for a majority of validators, constituting 51% or more, to provide their approval. The majority of the voting methods consist of block production and butler candidates. The researchers reached the determination that POV, which is a decentralized consensus algorithm, ensures minimal energy consumption, transactional certainty, robust security, and the prevention of blockchain forks.

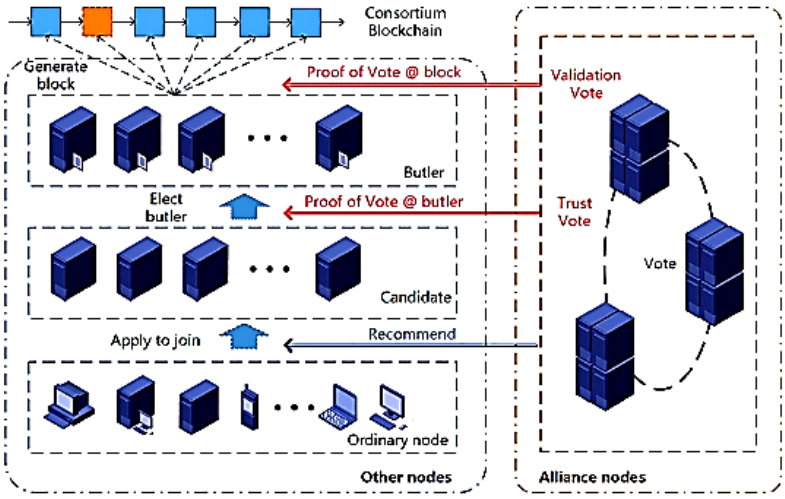

Fig 2. Two types of Proof of Vote

Fatrah, El Kafhali, Salah, and Haqiq [6] introduced a transparent blockchain-based ballot box system designed specifically for electronic voting. The protocol preserves fundamental attributes of electronic voting, as depicted in **Table 2**.

Table 2. Characteristics of E-Voting

Fairness	The outcome of the voting process will be revealed only after its conclusion, ensuring that the results remain inaccessible at any point. This measure is used to ensure that voters are not affected by the outcome.
Eligibility	The act of voting should be restricted to those who meet the criteria of eligibility, and each qualified voter should have the opportunity to cast their vote only once.
Privacy	The disclosure of voters' identities should be avoided throughout the process.
Verifiability	This feature ensures that all relevant parties have the capacity to check whether their votes have been counted or not.
Coercion-resistance	The detection of a forced voter's cast vote should be prevented from being discernible by the coercer.

Furthermore, voters are given the chance to modify or nullify their votes within a certain timeframe, and the system exhibits a degree of decentralization. The proposed protocol was successfully deployed on a closed network using the Ethereum blockchain application programming interface (API). It was established that a certain level of centralization was necessary in order to effectively achieve the primary objective. In order to mitigate the risks of impersonation and uphold the voting process integrity, the establishment of a Central Authority becomes imperative as a result of the inherent constraints of the public blockchain in safeguarding private data. The aforementioned process consists of four distinct voting sessions.

Initialization phase

Currently, the Constitutional Assembly (CA) has been designated, the regulations governing the electoral process have been formulated, and the blockchain technology, along with other pertinent systems, have been activated. The CA is provided with a roster of individuals who have officially registered as voters, together with a mechanism for authenticating the identity of these voters. In the context of the public signature scheme, a collection of signing and verifying keys will be generated, where the verifying key will be disclosed as a parameter applicable to the whole system. The genesis block alludes to the first block that is generated at the inception of a blockchain system. The validating key of the CA is included into the starting block, together with details pertaining to the set of valid nominations for the election.

Preparation phase

At present, the voter is required to use the client application of the e-voting platform in order to authenticate their identity to the CA. The CA utilizes the authenticated voter list and the data collected during the initialization process to ascertain the

eligibility of a voter to exercise their voting rights. Once the eligibility of the voter has been validated, the voter's client creates a public key pair. This public key serves as the voter's pseudonymous identity and verification key.

Voting Phase

During this particular stage, every individual participating in the voting process casts their vote and transmits it across the network. The vote will only be tallied and added to the block if the person has not yet cast their vote. In order to ensure the validity of a vote, it is necessary to verify that the ballot has been duly certified by the designated certifying authority (CA) and adheres to the prescribed format as stipulated. Individuals who use their right to vote via the amendment ballot possess the opportunity to rescind their prior votes. Multiple cancellations of a ballot are feasible, with only the most recent cancellation being included in the final result.

Counting Phase

During this stage, individuals are required to reveal their ultimate choice by transmitting a ballot opening message to the network. This message should include their voter ID for the final vote, the opening value of their vote commitment, and a signature for both values. After the completion of signature verification, voters go to declare the results to their neighboring individuals and proceed with the process of counting the votes. It is expected that all individuals inside a peer network would get identical outcomes, given their use of a shared blockchain infrastructure. The validity of the characteristics was established by protocol analysis. The protocol was seen to possess properties pertaining to eligibility, privacy, fairness, and verifiability, both at the individual and global levels.

IoT Management

The Internet of Things (IoT) has been formally described as a worldwide framework for the information society, enabling sophisticated services via the interconnection of physical and virtual objects. This interconnection is made possible by using current and developing compatible information and communication technologies.

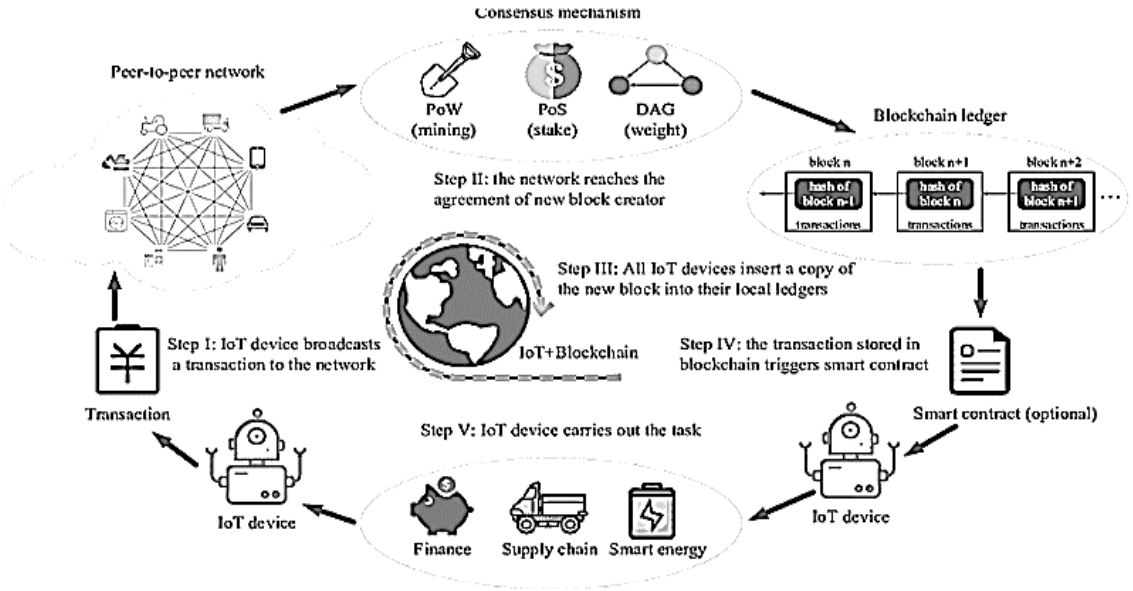

Fig 3. An example of Implementing Blockchain in IoT System

Numerous prospective solutions and initiatives have already emerged across various areas, with a particular emphasis on the incorporation of blockchain and Internet of Things (IoT) technologies, which now has a prominent position on the corporate agenda. The scholarly article by Agi and Jha [7] introduces a supply chain model that leverages blockchain technology. Within this particular configuration, the blockchain data has the capability to document and store information pertaining to the current state of delivered containers. As seen in **Fig 3**, a consensus mechanism plays a pivotal role in blockchain-enabled Internet of Things (IoT) systems by establishing a connection between raw data at the infrastructure level and the authenticated information required for executing diverse applications. This study aims to provide light on the inherent challenges associated with the development of a consensus mechanism for blockchain-enabled Internet of Things (IoT) systems.

Oviedo et al. [8] have shown advancements in mobility and accessibility. Parallelism is a rhetorical instrument, which integrates repetition of grammatic patterns or structures in a sentence or a series of sentences. In addition, the fourth aspect to consider is mass, while the fifth aspect pertains to scalability. Furthermore, the sixth factor to consider is openness. When comparing with other approaches for establishing a cohesive system. The solution leverages the capabilities of the Ethereum platform. The system has six primary components shown in **Table 3**.

Table 3. Components of the Ethereum Platform	
Wireless Sensor Networks	A communication network is used to achieve minimal power connection in applications with constraints.
Managers	An organizational body responsible for overseeing and regulating access privileges to Internet of Things (IoT) devices.
Agent Nodes	A node responsible for overseeing the implementation of intelligent contracts.
Smart Contracts	The inclusion of this component is crucial to the overall functionality and operation of the access control system.
Blockchain Network	A network based on a private blockchain.
Management Hubs	The interface facilitates the conversion of CoAP messages into JSON-RPC messages.

Williams [9] successfully addressed the c. A proof of concept (PoC) version of the distributed access control model was constructed to validate and analyze its functionality. The individuals developed their own blockchain based on Ethereum and used a universally accepted genesis block as the foundation for their application. In order to maximize the precision of the test outcomes, the designers and developers of the prototype made the decision to use a private blockchain instead of a public one. Nevertheless, the primary objective of my implementation was to use it in practical situations using publicly accessible blockchains. The current configuration is the integration of the intelligent contract inside the framework of a contractual account, while all administrative accounts are managed outside. The smart contract has two separate data structures that store the protected system data, manager data, and access control policy information. The term "mapping" refers to the data structure used for the purpose of storing information. Mapping structures, akin to hash-tables, are capable of storing several values for a set of possible keys simultaneously. The integration of diverse data sources into a cohesive entity may be achieved via the practice of mapping.

The interface leverages the web3 JavaScript API and the node-coap5 CoAP JavaScript library to create connectivity with the Internet of Things (IoT) and enable remote procedure call (RPC) communication between nodes on the Ethereum network and devices inside the network. The LibCoAP has been enhanced to enable automated generation of unique public/private key pairs by any system. The key used in the administration system is of a length of 20 bytes, serving the purpose of labeling machines. The library provides both a client and a server for the Constrained Application Protocol (CoAP). The study conducted in this evaluation used a laptop equipped with Ubuntu-16.04 operating system and an i7-950 CPU running at a clock speed of 3.07GHz.

The development of the Ethereum protocol included the use of Docker11 and a specific image known as vertigo/ethereum12. This image was constructed from the client-go image, which is an implementation of the Ethereum protocol in the Go programming language. In addition, Vertigo underwent several modifications to enhance the administration of a private Ethereum network. All Internet of Things devices were using the most recent version of the LibCoAP library. The execution of CoAP has been performed using a benchmark tool called CoAPBench13, with Californium14 serving as its reference point. Based on the cited source, it can be argued that CoAPBench is the only feasible method for doing benchmarking in the context of CoAP.

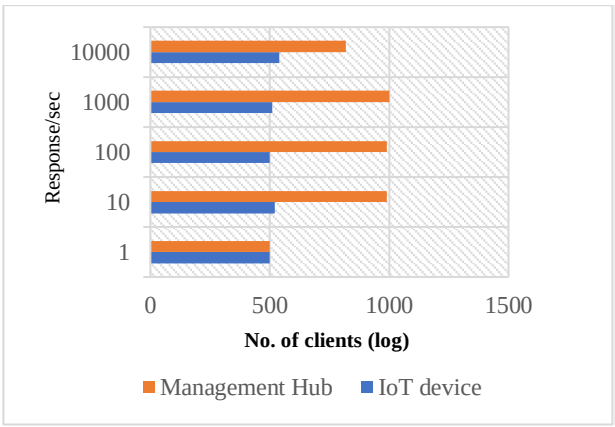

Fig 4. Within the context of a management hub and an IoT system, the process of obtaining information from the management hub is carried out independently, resulting in a measure of throughput.

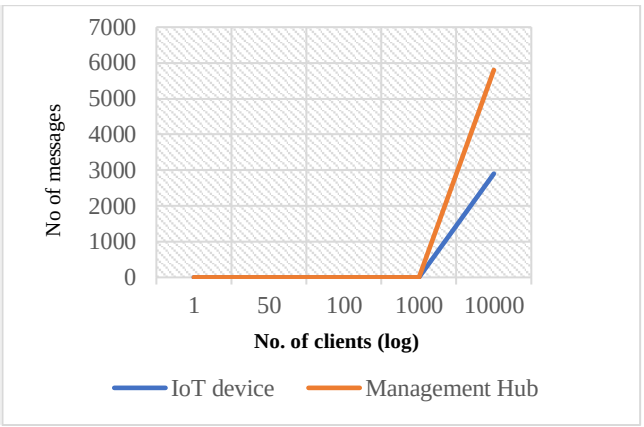

Fig 5. The number of test timeout inquiry messages performed in Fig 4.

Fig 4 and **Fig 5** provide a preliminary estimate derived from the original study. In their study, Francesco et al. (5) have examined a model known as the Tweet-Chain, which has a comparable level of anonymity to that of the Blockchain. The approach they propose offers an alternate means for the construction of a public ledger. The proposed concept aims to revolutionize the consensus protocol by using tweets, so replacing the traditional elements of Proof of Work (PoW) and

miner fees. This approach effectively addresses the limitations associated with limited processing power and storage capacities, making it well-suited for applications in the Internet of Things (IoT) domain.

The organization has a total of three individuals that serve as performers. The Twitter social network provides registered users with the capability to post, monitor, and notify others of tweets, along with a user-friendly profile interface. The purpose of its implementation was to provide a kind of directory service known as the Tweetchain group, which included a collective of users, denoted as C, who actively participated in the use of the Tweetchain protocol. The user begins their participation in the Tweetchain community by generating a SHA-256 hash chain of length k, starting with a password. This chain would serve the purpose of maintaining the interconnectedness and immutability of all the activities inside his period. Buccafurri, Lax, Nicolazzo, and Nocera [10] also discovered that the system is in a state of stability. This implies that inside the Tweetchain group, there exists a minimum of $s = \frac{2t}{1-m}$ participants, where t and m represent system parameters.

The process of registration involves a prospective member, denoted as x, who wishes to join the C group of Tweetchain. The next step in establishing a presence on Twitter is undoubtedly obtaining a standard membership to the platform. Hence, in a join-first chronology, the set W consists of a minimum of one tweet per member. At this juncture, x generates the F(x) set in a random manner, consisting of follow-up actions selected for the purpose of verifying its transactions in the future. The Fx set is constructed in the following manner:

- The individual, denoted as "x," is in search of the unique identification associated with their Twitter account. Each Twitter account is assigned a unique identity consisting of 64 bits.
- The identifier serves the purpose of generating random integers that act as a seed for a public pseudorandom number generator (PRNG). The value of n mod w is calculated for each produced number, whereas w represents the overall tweets by W, correlating the Tweetchain community.
- The user's text does not comprise of any data to rewrite. The obtained values are used as indexes to choose various profiles of W.
- The user's text does not contain any information to rewrite. During this phase, x initiates individual communication with each account, sending them a private message with an invitation to join him.

The user's text does not present any data to rewrite in an academic format. Each of the considered methods incorporates the inclusion of a hyperlink to x by verifying the authenticity of the incoming message from x via the utilization of the group PRNG. Additionally, the method involves duplicating the introductory tweet of W by making alterations to the hashtag #HCWi with the current hash chain. The term "feature" refers to a distinctive characteristic or attribute of a particular entity or object

The process of generating transactions

This is the protocol implemented to initiate a novel transaction. Similar to Blockchain, many data elements are used in each transaction, including a timestamp indicating the time of the transaction, a payload representing the core content of the transaction, a transaction with input, and a collector of sales, which refers to a target profile. The process of generating a new transaction in this method pertains to the posting of a user's most recent tweet. This social media post is referred to as a tweet.

Verification

This methodology has been used to authenticate the authenticity of a transaction. This process does not acknowledge the verification of a transaction material. The connection between the subject matter and the purpose of the contract is exclusively determined by the contractual intent, which is wholly dependent on the implementation and unrelated to the proposal. A Java prototype was developed, which included this technology, and all the experimentations were done on an individual computer composed on Intell17 Processor unit that is on an operational sped of 4 GHz and devices composed on 8 GB of RAM. The operating system containing Ubuntu 16.10 was equipped with JDK, Apache, and Tomcat servers in terms of the applications implemented.

In summary, the duration required for the verification process of a t-tweet was 13.5 units of time. Therefore, the efficacy of this strategy surpasses the present condition of art. Within Blockchain, the average time interval is around 10 minutes, depending upon the charge paid. Conversely, in Ethereum, under optimal circumstances, this interval is reduced to approximately 15 seconds, particularly when the verification of participation is considered crucial. In their study, Kaur et al. [11] have presented a methodology that focuses on enhancing the security of Internet of Things (IoT) devices within the context of a smart home environment, using blockchain technology. The methodology used by the researchers comprises a series of hierarchical levels. The first topic of discussion pertains to cloud storage, while the second topic concerns overlays. The concept of a "smart home" refers to a residential dwelling that is equipped with many interconnected devices and systems that are capable of automating and enhancing the functionality and efficiency

Every smart home is equipped with a central processing unit that manages the transmission of data both inside and externally. Every miner is consistently connected to the network and has enough resources. The miners play a crucial role in maintaining the confidentiality and integrity of a blockchain system. Isnaini and Suhartono [12] have successfully shown a robust framework by conducting a comprehensive investigation of the principles of secrecy, availability, and integrity.

Supply Chain Management

A supply chain refers to the interconnected system of companies and suppliers collaborating to produce and distribute goods or services to end customers. The diverse array of individuals, collectives, institutions, endeavors, assets, and information that constitute this interconnected network. The primary functions executed by a supply chain include the generation and dissemination of items, promotion of those products, financial management, operational oversight, and provision of customer assistance. Supply chain management refers to the systematic coordination and control of the many activities involved in the manufacturing and distribution of goods and services. This process encompasses the acquisition of raw materials and culminates in the delivery of the completed product to the end consumer.

The implementation of supply chain management has a vital obligation in optimizing the production cycle and minimizing costs within a contemporary supply chain. Supply chain management facilitates the reduction of inefficient production expenses and the timely fulfillment of deliveries for enterprises due to its centralized structure. When applied to the domain of blockchain technology and supply chain management has the capacity to enhance transparency, augment traceability, alleviate the weight of risk and operational costs, and eventually enhance financial gains. There are many other benefits associated with implementing a blockchain-based supply chain. These include a reduction in losses resulting from counterfeit market transactions, streamlined administrative processes with less paperwork, enhanced legitimacy and trust in the supply chain, and increased stakeholder involvement.

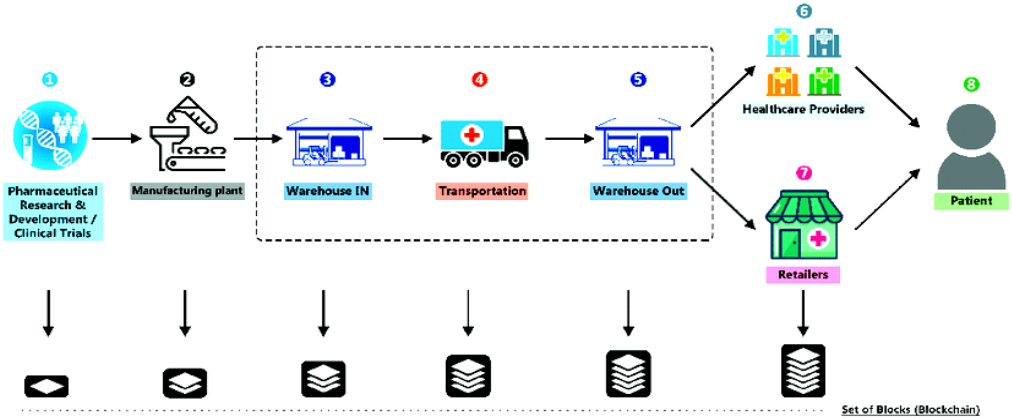

Fig 6. Supply Chain Management in Blockchain

Fig 6 depicts a pharmaceutical supply chain management (SCM) method that utilizes blockchain technology. The diagram has been explained using steps 1 to 8, in **Table 4** below.

Table 4. Steps of SCM tased on Blockchain Technology

Step 1	The first step in the development of a novel drug or medical treatment involves the establishment of a legal framework, including patent protection, as well as the initiation of a lengthy series of clinical studies. The aforementioned data is documented inside the digital ledger as a means of conducting a transaction.
Step 2	In the second phase, after the successful completion of the clinical study, the patent is transferred to the manufacturing facility for the purpose of conducting test prototyping and initiating mass production. Every product has different form of identity, which is seamlessly included into a block and transaction within blockchain, including pertinent details.
Step 3	In the third step of the process, after the completion of mass manufacturing and packing, the medication is collected and stored in a warehouse in reaction to additional distribution. Blockchain incorporates several pieces of information, including but not limited to lot number, time, expiration date and barcode.
Step 4	The blockchain includes transport details, including the duration of movement between warehouses, the authorized agent, chosen method of transportation, and other relevant information.
Step 5	In the fifth step, pharmaceuticals and clinical supplies to medical practitioners or merchants is often entrusted to a third-party network of distribution. A dedicated warehouse is used for each third party, serving as a central hub for connecting all distribution terminals. In addition, the blockchain incorporates a distinct transaction.
Step 6	In order to verify and avoid counterfeit, care givers such as clinics, and hospitals have to provide pertinent data, including but not limited to lot number, batch number, expiration date, and product owner. Furthermore, this data is integrated within blockchain.
Step 7	The acts undertaken by a store are analogous to those in Step-6.
Step 8	The patients are advised to actively ascertain the legitimacy of products throughout the whole process, as the application of blockchain within supply chains provides transparent information that can be used for verification purposes by prospective purchasers.

According to Moosavi, Naeni, Fathollahi-Fard, and Fiore [13], there are three distinct use cases of blockchain technology in the context of supply chain management. 1) The use of traceability mechanisms facilitates the optimization of operational efficiency by means of mapping and visualizing company supply chains. The application of blockchain could facilitate and guarantee the interaction and involvement of organizations and customers by using data that is unchangeable and can be verified. 2) Tradeability is a distinctive feature of blockchain that revolutionizes the idea of conventional marketplaces. The process of tokenization involves the division of an asset into digital shares, which are used to represent and establish ownership. This is achieved via the use of blockchain technology.

The aforementioned tokens have the capability to be exchanged between individuals, hence facilitating the transfer of ownership. Transparency is a crucial aspect that fosters confidence by documenting significant data points such as claims and certifications, which are then made available to the public. Certain supply chain startups, such as Provenance, employ blockchain technology to monitor and trace the responsible sourcing of tuna in Indonesia. Additionally, Monegraph [14] utilizes blockchain to safeguard the utilization and dissemination of digital media rights, while facilitating the equitable distribution of revenue among distributors, publishers, and creators in the media industry.

Identity Management

The process of identity verification often involves the submission of paperwork, along by the provision of further personal information. The use of a driver's license as a means of identification may potentially expose personal information pertaining to the individual in question, including their place of residence, eye color, height, and hair color. The potential consequence of this data is the unauthorized acquisition of an individual's identity. Identity theft, often known as the illicit use of an individual's personal information without their consent, has emerged as a burgeoning issue in the contemporary era of digital technology. Current identity verification methods include limitations in ensuring data security, which can only be guaranteed to a limited extent. In the realm of online identity verification, passwords and, at times, two-factor authentication are used.

In contrast to dual-factor authentication, which often use a one-time password or a third-party entity, password-based authentication depends only on passwords, which are well recognized for their inherent vulnerability. Given its decentralized nature, blockchain has the potential to address issues associated with the conventional verification process. The storage of data in a decentralized ledger may enhance security measures, hence increasing the difficulty for unauthorized entities to get access. Due to the decentralized nature of the ledger, an adversary would need to successfully breach all computers inside the network in order to illicitly acquire or modify any data.

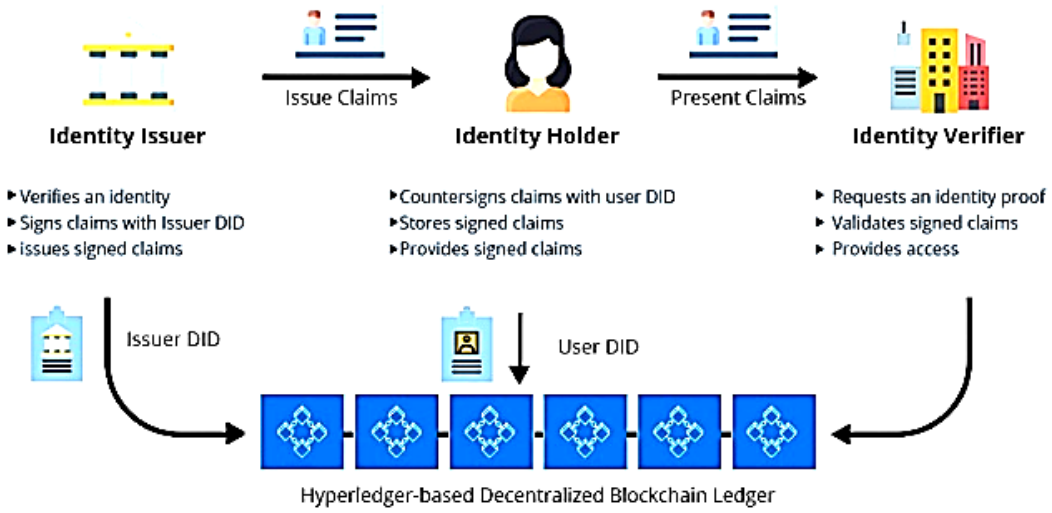

Fig 7. Identity Management Framework Using Blockchain

According to the illustration shown in **Fig 7**, authorized issuers have the capability to provide identity owners with confirmed credentials, therefore granting them access to identity information. The KYC data will include the user's identifiable information as shown in their confirmed credentials. The QR code contains a compilation of entities responsible for issuing a particular item, and a verification template has been devised to accurately identify and highlight the pertinent information.

In their study, Nanayakkara, Rodrigo, Perera, Weerasuriya, and Hijazi [15] conducted an analysis of the methodologies used by companies such as Blockstack and Tierion in the realm of user identity management and verification. The process of authentication involves the use of a handshake mechanism based on the blockchain technology employed by Blockstack, which encompasses the authenticating app, user, and third party. When a user endeavors to get access to an application that requires a password, they initiate the first stage of this authentication process by sending an authentication request. In this

scenario, the user will not be required to provide a password for authentication purposes. Instead, they will encounter a username form inside the secure application. Subsequently, the user will be provided with a QR code for authentication, or another authentication method will be used. The subsequent step in the handshake process involves the verification of the request and the subsequent provision of a response.

The aforementioned procedure has many steps in order to ensure the attainment of authenticity. The legitimacy of the request may be verified by using public key cryptography. then, the protected application has the capability to digitally sign the request, which may then be subjected to public verification by either the blockchain or the certificate authority. Once the verification process has been completed, the user will be prompted to click on the "verify login" button. Once the user has generated and authorized the request, it is then sent back to the secure application through a designated pathway. Access will be allowed to the user after the secure application has verified their request via the use of public key cryptography. Tierion utilizes cryptographic hashing techniques in order to guarantee that just essential data is sent.

The user employs cryptographic hashing and digital signing techniques to secure a data packet containing relevant information prior to transmitting it to the website for the purpose of authentication. Upon ascertaining the hashed and signed representation of the data, this website proceeds to search for it inside the blockchain. If the cryptographic hashes are congruent with the digital signatures, the website will ascertain the veracity of the data's association with the individual and its integrity, therefore ensuring that the information originates from the authorized user. The use of methods employed by Blockstack and Tierion has the potential to establish a robust and decentralized framework for the authentication and verification of identity, including a wide range of functionalities while ensuring a high level of security.

The Identity system, as proposed by Liu, He, Obaidat, Kumar, Khan, and Raymond Choo [16], employs blockchain technology as a means to document and authenticate an individual's credentials and other pertinent identifying details. The ability to monitor and ascertain individuals with authorized access to their personal information is facilitated by the inherent security mechanisms of blockchain technology. Within the newly implemented system, there are three distinct categories of users: normal users, administrators, and those external to the system. The user provides consent for a third party to get its data and may see the roster of entities making such requests. The entity in charge has the capability to upload the user's personal information into the blockchain, while the third party initiates the request to access the user's data. The Agile Unified Process was used in the development of their system. There were four discrete phases of implementation.

During the first phase, the system's limitations and parameters were defined, and the critical components were identified. The study also examined the security problems and inefficiencies inherent in the existing approach. The subsequent phase included the development of the system design via the use of six Unified Modeling Language (UML) diagrams. The system's third version was developed using Android 3 and Microsoft Visual Studio Code, which served as a hybrid mobile and web application development platform. During the final phase, an evaluation was conducted on the operational aspects of the proposed system via the implementation of system testing and acceptability testing. A comprehensive analysis was performed on a set of 18 case scenarios. The acceptance assessment included three primary criteria: 1) a desire for online verification, 2) the ease of doing online verification, and 3) ensuring accessibility. Out of a total of 141 respondents, 65 individuals expressed a preference for online verification. Additionally, 116 participants affirmed that the system provides a straightforward verification process, while 109 respondents advocated for universal accessibility to the system. The researchers argued that by using the current blockchain technology, the system will serve as a proficient tool for managing identities.

The [17] proposed the use of the Ethereum blockchain as the foundation for an identity management system. The blocks were used to securely store the personal data of people, while also integrating identity authentication and reputation control mechanisms [18]. The distributed ledger architecture of blockchain renders the stored information impervious to control or manipulation by any centralized entity. The blockchain development environment Testrpc, the smart contract framework Truffle, and the programming language Solidity have been used by the individuals. In order to illustrate its functionality, the system has been deployed on a blockchain network including a limited user base consisting of a total of ten individuals.

The suggested system is unique in its combination of integrated identity authentication and reputation management components, since no previous system has shown such features. The major objective of the identity authentication module is to ensure that virtual identities generated on the system are exclusively associated with real-world entities, achieved via the correlation of the identity with the Ethereum public key. Conversely, the primary objective of the reputation management division is to monitor and assess user behavior inside the system. The authentication model has two distinct components. The discourse delineates two distinct categories of modifications to an individual's identity. Given the absence of a constraint on the quantity of Ethereum public key addresses that may be produced, it becomes feasible for an assailant to influence reputation outcomes by assuming false identities.

III. CONCLUSION AND FUTURE DIRECTIONS

Due to its inherent attributes of decentralization and trustworthiness, which render it autonomous from centralized governing bodies, blockchain technology has rapidly gained widespread adoption within the realm of information systems. Despite the widespread adoption of blockchain in different industrial segments such as supply chains, finance, healthcare, education, and energy consumption, aimed at enabling the development of Internet-based distributed databases, the existing body of research on this subject remains limited to a few preliminary investigations. Hence, it is fundamental to examine the present condition of blockchain technology within the financial sector, with a specific emphasis on the potential ways in which

blockchain designs might facilitate the attainment of a competitive advantage for the industry. This article provides a comprehensive analysis of many blockchain applications, including voting methods, IoT, supply chains, and identity management. While acknowledging the merits of these applications, the research eventually asserts that blockchain technology is not devoid of limitations and raises concerns over its reliability. The dependence on a reliable third party in the development of several applications may contradict the decentralized principles inherent in blockchain technology. Nevertheless, blockchain has attributes such as transparency, security, traceability, tradeability, privacy, and data auditability that, if effectively harnessed, have the potential to instigate a paradigm shift in the realm of technology. Given the nascent stage of blockchain technology and the limited number of validated applications, coupled with the absence of operational instances at now, it is expected that a surge of novel innovations and concepts will emerge in the foreseeable future.

Data Availability
No data was used to support this study.

Conflicts of Interests
The author(s) declare(s) that they have no conflicts of interest.

Funding
This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT (No.2022R1F1A1063340)).

Ethics Approval and Consent to Participate
The research has consent for Ethical Approval and Consent to participate.

Competing Interests
There are no competing interests.

References

[1]. Weforum.org. [Online]. Available: https://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf. [Accessed: 20-Aug-2023].
[2]. S. Tanwar, "Decentralization and architecture of blockchain technology," in Studies in Autonomic, Data-driven and Industrial Computing, Singapore: Springer Nature Singapore, 2022, pp. 63–81.
[3]. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," Sensors (Basel), vol. 21, no. 17, p. 5874, 2021.
[4]. A. Mukherjee, S. Majumdar, A. K. Kolya, and S. Nandi, "A privacy-preserving blockchain-based E-voting system," arXiv [cs.CR], 2023.
[5]. K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2017.
[6]. A. Fatrah, S. El Kafhali, K. Salah, and A. Haqiq, "Transparent blockchain-based voting system: Guide to massive deployments," in Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, 2021, pp. 237–246.
[7]. M. A. N. Agi and A. K. Jha, "Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption," Int. J. Prod. Econ., vol. 247, no. 108458, p. 108458, 2022.
[8]. D. Oviedo et al., "Accessibility and sustainable mobility transitions in Africa: Insights from Freetown," J. Transp. Geogr., vol. 105, no. 103464, p. 103464, 2022.
[9]. C. C. Williams, "Explaining the informal economy: An exploratory evaluation of competing perspectives," Relat. Ind., vol. 70, no. 4, pp. 741–765, 2016.
[10]. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Tweetchain: An alternative to blockchain for crowd-based applications," in Lecture Notes in Computer Science, Cham: Springer International Publishing, 2017, pp. 386–393.
[11]. B. Kaur et al., "Internet of Things (IoT) security dataset evolution: Challenges and future directions," Internet of Things, vol. 22, no. 100780, p. 100780, 2023.
[12]. K. N. Isnaini and D. Suhartono, "Evaluation of basic principles of information security at University using COBIT 5," J. Matrik, vol. 21, no. 2, pp. 317–326, 2022.
[13]. J. Moosavi, L. M. Naeni, A. M. Fathollahi-Fard, and U. Fiore, "Blockchain in supply chain management: a review, bibliometric, and network analysis," Environ. Sci. Pollut. Res. Int., 2021.
[14]. "How monegraph uses the block chain to verify digital assets," Monegraph, 21-May-2021. [Online]. Available: https://www.monegraph.com/how-monegraph-uses-the-block-chain-to-verify-digital-assets/. [Accessed: 20-Aug-2023].
[15]. S. Nanayakkara, M. N. N. Rodrigo, S. Perera, G. T. Weerasuriya, and A. A. Hijazi, "A methodology for selection of a Blockchain platform to develop an enterprise system," J. Ind. Inf. Integr., vol. 23, no. 100215, p. 100215, 2021.
[16]. Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: A review," J. Netw. Comput. Appl., vol. 166, no. 102731, p. 102731, 2020.
[17]. A. R and A. H, "Advantages, Methods and System Architecture of Spectral Imaging in Biomedical Engineering," Journal of Biomedical and Sustainable Healthcare Applications, pp. 51–58, Jan. 2022, doi: 10.53759/0088/jbsha202202007.
[18]. C.-G. Koa, S.-H. Heng, and J.-J. Chin, "ETHERST: Ethereum-based public Key Infrastructure identity management with a reward-and-punishment mechanism," Symmetry (Basel), vol. 13, no. 9, p. 1640, 2021.