

**Analysis of Publications on Applications of Blockchain Technology**

**INSE 6120: Cryptographic protocols and Network Security**

**Presented to:** Professor Ivan Pustogarov

Mirza Aliva Salvin **40198142**

Md. Aminul Islam **40203451**

Saif Manjar Ahmad **40217056**

Taufiq Al-Din **40217260**

Kareem Shamayleh **40222388**

**Abstract—** The military, the Internet of Things (IoT), video games, NFTs and banking are just a few of the many areas where blockchain technology can be used. The survey looks into the challenges and limitations, potential advantages of blockchain technology in these areas, and current research and development. In the military, blockchain innovation can possibly upgrade the security and straightforwardness of military tasks and supply chains. The survey looks at the advantages and use cases of blockchain in the military, as well as the difficulties associated with its implementation. Blockchain technology can aid in the development of secure, decentralized networks for the exchange of data among IoT devices. The survey investigates the current state of research and development in this field as well as the potential uses of blockchain in the Internet of Things. The video game industry is also incorporating blockchain technology more and more, particularly in the areas of digital asset ownership and trading. The survey looks at how blockchain is used in video games and how it helps players and game developers. The review additionally examines the utilization of non-fungible tokens (NFTs) and blockchain in banking. The survey looks at how NFTs could be used in banking and financial services because they are being used more and more in the arts and entertainment sectors. Overall, this survey provides an overview of the current state of research and development in the areas of banking, the Internet of Things, video games, the military, NFTs and blockchain technology's potential benefits and drawbacks.

**Keywords—** Blockchain in Military, IoT, Video Games, NFTs, Blockchain in Banking.

# I. INTRODUCTION

**B**lockchain technology's rising popularity may be attributed to its promise of reliable, immutable, and decentralized record-keeping. Financial institutions are among the most visible adopters of blockchain technology. Financial transactions conducted using a blockchain-based payment system are faster, more secure, and have lower transaction costs. Smart contracts built on the blockchain can automate the implementation of agreements, further cutting down on the need for middlemen while increasing the efficacy of financial transactions. Blockchain has the potential to increase the military's efficiency and effectiveness by bolstering the safety of communication, data storage, and supply chain management. Internet of Things (IoT) gadgets are another potential use of blockchain technology. By facilitating a trustless and encrypted network for IoT device-to-device interaction and data sharing, blockchain has the potential to significantly enhance the robustness and safety of IoT infrastructure. Several industries may benefit from this, including smart buildings, transportation, and healthcare. The video game sector is likewise investigating blockchain's possibilities. Blockchain technology may facilitate safe and transparent transactions in online gaming, improving the trustworthiness and efficiency of buying, selling, and trading in-game items and currencies. Moreover, blockchain technology might pave the way for the development of non-fungible tokens (NFTs), which are singular digital assets that can stand in for the ownership of digital artwork, music, and other forms of creative output. Blockchain technology has a lot of potential uses in several sectors, and it might help companies and governments overcome a lot of their existing problems. More creative applications of blockchain technology are likely to emerge as the technology develops and advances.

In this project report, we will study many publications/projects that use blockchain technology as the underlying technology. To do this, we have opted to have each member perform research on a separate subject in which blockchain technology was utilized.

# II. BLOCKCHAIN MECHANISM

Blockchain is a distributed ledger that keeps records of transactions in a way that is both immutable and visible. Each block in the chain includes a cryptographic hash of the prior block, making for a secure and unalterable ledger of all past transactions. Each new transaction is added to a block when it is validated by the network of computers (nodes). As a new block is added to the blockchain, a notification is sent out throughout the network and every node updates its own blockchain to reflect the change. This results in a decentralized system in which no one party controls the flow of data or the actions of the other members. Participants are motivated to contribute to the network to maintain the integrity of the blockchain via the use of a consensus mechanism, which is the process by which nodes in the network agree on the correctness and chronological order of blockchain additions. Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated Proof-of-Stake (DPoS) are all examples of consensus procedures (DPoS).

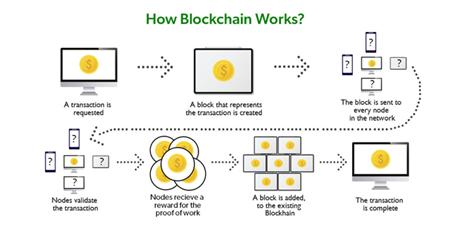


Figure 1: Blockchain Mechanism[1]

In a Proof-of-Work system, miners compete to use a very powerful computer to solve a difficult mathematical challenge. The first miner with the correct answer will notify the network, and the rest of the network will check their work. If the miner's answer is accepted, they will get a portion of the freshly minted bitcoin. Using PoS, users are selected to verify transactions in proportion to the quantity of bitcoin they own. It follows that the greater a user's holdings of bitcoin, the more likely they are to be selected to authenticate transactions.

As a decentralized, secure, and transparent ledger system, blockchain technology has the potential to significantly alter several markets. We anticipate that as blockchain develops further, new, and creative applications will emerge

# III. BLOCKCHAIN IN THE MILITARY

## Military Blockchain for Supply Chain Management [2]

### Literature Review

In this article the authors describe the importance of supply chain management, especially in military parts transportation. The article begins with a simple explanation of what supply chain management (SCM) is and what blockchain is and how both can be integrated. Supply chain management, as described in the publication, is the process of production and distribution, it is a system in which we ensure the transportation of raw materials from a supplier until it is delivered to the end customer as a final product. In the middle of it all the raw materials have been presumably processed into parts and those parts put together to create the final product.

The publication also mentions issues pertaining to SCM, especially in the vein of counterfeiting, incompetence, missed parts, etc... Along with this it mentions the unreliability of keeping track of issues like these with normal SCM systems, this can be addressed with the traceability that Blockchain technology provides. It would enable anyone to track an error back to its source due to its meticulous nature which will be explained soon.

Blockchain technology as described in its essence is a decentralized ledger of transactions built into a network, transactions are conducted over the network using whichever protocols the network implements and saves this transaction on a “chain” and it is saved on every machine in the network, normally referred to as “nodes”. As the transactions go through every node the system facilitates the recording of each state of this transaction. You can figure out how this kind of system is virtually impenetrable to counterfeiting as each node would have to be verified for something within the transaction to be edited.

Only few military defenses are exploring the need for blockchain technology due to the tech’s secure nature, according to the article there are seven possible cases for blockchain technology to be applied for military defense:

1. Tracing Defense Shipments and Contracts.
2. Secure government and battlefield messaging.
3. Cyber warfare preparedness.
4. Preventing data theft.
5. Protecting weapons systems.
6. Military additive manufacturing.
7. NATO applications.

The publication will focus mainly on the 1st application, in the case for military SCM, it is a complex matter, unlike privatized SCM.

The proposed framework in the paper is for Navy defense shipments, even though it is called the Navy it does not handle only sea operations, therefore Navy shipments need to be put under a good amount of scrutiny and need to be ready when needed. In the case of managing part transportation for ships for example, parts need to be genuine to ensure the assets are functioning properly, and constant contact needs to be made to suppliers to assure punctual deliveries as delays will affect the overall vessel completion, that’s why traceability is an important part of this SCM.

Diagram

Description automatically generated

Figure 2: Blockchain recommendation for the Navy SCM[2]

The above figure is the proposed blockchain adaptation to the Navy SCM, As you can see it includes three parties that need to keep communication constant, the supplier which sends the parts/raw materials, the traceability provider which keeps track of each shipment made as well as how long each shipment remains in each branch, and finally the destination or in this case it is named “Depot in RNM”. This proposed project will be closed off only to the military to prevent outside interference, communication will be encrypted within the blockchain, and a ledger will be produced to keep track of all shipments, and a Navy depot known as “West Fleet Supply Depot” will act as an appraiser to assure the authenticity and functionality of the parts.

This specific blockchain like all others keeps a ledger at each node that gets updated with each transaction, but uniquely it allows the navy depot to give read, write, and delete, it is applicable here due to the sensitive nature of military information. When a new transaction happens the node at which this transaction occurs produces a proof of work document and broadcasts it to all other nodes, the other nodes will verify the information and validate the transaction, once it has been validated it will be written into the blockchain.

The publication concludes by reiterating how this kind of SCM will have genuineness in its dealings and it is secure due to all nodes being involved in the information exchange, the author then emphasizes how this should provide a good motivation for integrating blockchain technology into military SCMs.

## Military Intelligence Applications for Blockchain Technology [3]

### Literature Review

This paper focuses on analysing various fields within the military as well as the blockchain itself, afterwards the researchers aim to see where blockchain would fit best and how this fit would vastly improve the field in which it was implemented in.

#### Military Intelligence Background

Military intelligence in the United States is the process in which information is collected, analysed and a decision is made based on this information, the below figure is provided by the publication, and it depicts the core tenets of intelligence.

Chart, funnel chart

Description automatically generatedFigure 3: Relationship between data, information, and intelligence[3]

It is stated that intelligence is the core of all operations within the military and the decisions made from data gathered through intelligence is what shapes the state of the military. Thus, the collection, analysis, and exploitation all need to be efficient and effective to help create a better situation for a decision to be made. Military intelligence is growing fast, and many technologies are being researched as potential applicants to the process, such as artificial intelligence vis-à-vis Project Maven[4] which is working on integrating A.I and machine learning to Military intelligence. Much more requirements are being made to leverage new technology to aid the U.S military and blockchain should be one of them.

#### Blockchain Background

Blockchain technology works in terms of blocks of data chained together in a way such that any alteration to a block will cascade through the chain and alter subsequent blocks, how this works is that the first entry in a block is usually the previous’ block cryptographic hash value, this helps in preventing malicious alterations to the chain. There is also a distributed ledger sent to all the users within the chain, the decentralized nature of this ledger makes it so that if a change happens every ledger with every user is also altered to reflect that change.

There are two ways the system solves the issue of having two different ledgers: proof-of-work (POW) and proof-of-stake (POS). POW: this method includes the use of nonces that will be hashed and be used as leading bits on the block, miners will usually hunt for these nonces and once a new one is found a block is finished and the miner will broadcast this to everyone else, in this case if a fork occurs (discrepancies in ledger data) the longest copy of the ledger will be used to represent the final ledger. POS: this method gives the power to the users with the most stakes in the network (i.e., the users with the most discovered nonces) to determine the consensus on the final ledger, thus most users will be racing to find new nonces to up their stakes.

#### Potential Applications

##### Big Data

With military intelligence there is a staggering amount of data flowing through the channels set up by defense projects, the sheer amount of data leads to a good amount of it being unreliable and maybe even irrelevant to the subsequent decision that needs to be made. The previously mentioned Project Maven and other automated learning software being applied to military intelligence creates a black box conundrum to the collected data.

Diagram

Description automatically generated

Figure 4: Blockchain technology used for preserving providence.[3]

In the above figure, blockchain technology is represented in a way that we can trace a decision made back to the intelligence collected that led to this decision. This helps in preserving data connections so that assessments of poor decisions or even acknowledgement of good decisions will be accurate, and the correct people are accountable for their actions.

##### Distributed and decentralized access

Intelligence systems of any military are constantly under fire from foreign attackers attempting to undermine the whole system, vulnerabilities that give way for these attackers to modify data, disrupt services, and deny access altogether. With blockchain an attacker's ability to penetrate a system using the technology is severely withering.

Blockchain can be used to protect databases to prevent loss of data due to its decentralized nature, however it can also protect computer software from having malicious code being inserted into it and gives nodes the ability to detect malicious attackers in the network.

##### Ethical Accountability

Due to blockchain’s auditable nature, the technology excels in being ethical, in a sense that if there is any malfeasance in the governments or the military’s activities, blockchain as mentioned multiple times allows for the tracking of information along the chain back to its source so the data can be audited with ease and will hopefully dissuade malicious actors from within.

#### Proposed design.

The authors propose a design around blockchain technology that best utilizes its potential, the authors reiterate how through their literature review almost every author agrees on the central point of attack defense that blockchain can give military intelligence. In wartime there are many ways an enemy faction can disrupt network services through exploiting cyber vulnerabilities, or even just attacking electrical systems, that’s why a decentralized distributed system will aid in retaining a semblance of system functionality even if the ledger has to fork in a way or two.

The authors agree that the permissionless blockchain variant is not well suited for military intelligence use (due to the hierarchical nature of any military) so a permissioned blockchain is the way to go. Stating this it is also agreed upon that when an activity requires a central figure to regain complete control of a service due to whatever reason, a decentralized blockchain may not work as “it is not congruent with applicable command philosophy and regulation”. The below figure illustrates more clearly what the authors intended blockchain technology to be used for in the military.

Text, chat or text message

Description automatically generated

Figure 5: Determining where blockchain technology fits within the military.[3]

A more specific design would be the proposed blockchain application to the AIS or Automated Identification System, this is a system used by the nautical branch of the military to keep track of all ships deployed within a given area. The system is very similar to cryptocurrency systems in which individuals within the system do not necessarily trust each other but they all have to cooperatively participate. The system would involve the AIS station receiving ship reports through radio, accumulating the reports with a frequency of over 1500 reports per minute and adding them to a block-creation process, afterwards the station would broadcast the changes it received to all other stations within its network. Below is a figure from the publication that illustrates this.

Diagram, text

Description automatically generated

Figure 6: AIS blockchain application.[3]

## Thoughts

Reviewing both publications shed a light on how blockchain technology can vastly improve some military activities, but we also discovered that unnecessarily applying technology where it is not needed can cause a waste of time and resources. The second article in particular went in depth on how not all branches of the military particularly need blockchain technology and the ones that do are usually dependent on information, in the vein of storing information, transferring information, analyzing the information and using the analysis to make a well-educated decision.

Regarding the first publication, I agree with the authors in that military SCM would greatly benefit from blockchain technology. SCM as mentioned before is a complicated process that involves countless steps, making it difficult to keep track of all the phases a shipment would go through, however with a blockchain implementation the process is much easily more auditable than before, any mistake can be traced back through all the phases to check for malpractice. The decentralized nature of the blockchain ledger also provides redundancy protection in case attackers would think of disrupting a node on the network (other nodes would have a copy of the ledger and the information would be preserved).

Regarding the second publication, the authors did not necessarily provide us with a specific application but rather a range of activities in the military that may be aided with blockchain technology. While we found this to be a bit inconclusive it helps in painting a bigger picture of blockchain use in the military, any process that could be vulnerable to centralization as well involving collecting and transferring intelligence, also similar to the previous publication the authors put an emphasis on the traceability and transparency of problems.

# IV. BLOCKCHAIN FOR IOT DEVICES[5][6][7][8]

The Internet of Things (IoT) is expanding quickly, but because of its fragmented topology and resource-constrained devices, it has privacy and security flaws. The proposed answer is the blockchain (BC) technology, however it is computationally expensive and has substantial bandwidth overhead, making it unsuitable for IoT. The new architecture suggested in this paper, which is based on BC technology, keeps most of the advantages of that technology's security and privacy while reducing overhead. The suggested architecture is hierarchical and consists of cloud storage that coordinates data transfers with BC, smart homes, and an overlay network. Depending on where a transaction happens in the network hierarchy, different forms of BC are used, and distributed trust techniques guarantee a decentralized topology. A case study of a smart home application demonstrates the usefulness of the suggested architecture in providing security and privacy for IoT applications under typical threat models.

The Internet of Things (IoT) makes it possible to collect data with great detail, which boosts productivity and delivers cutting-edge services but also poses major security and privacy risks. First-generation IoT products have been shown to have a number of security flaws, and the special properties of IoT, such as its scale, lack of central management, and various attack surfaces, make security and privacy issues even more difficult. Researchers have given these problems a lot of attention, but there are yet no complete solutions. In order to manage privacy concerns, regulate access to sensitive data, offer authentication and privacy, and ensure privacy-aware sharing of IoT data, new techniques are required. IoT security and privacy issues might be addressed by BC. Since blockchain is decentralized, there are no single points of failure, allowing for scalability and robustness. Blockchain also provides anonymity, making it appropriate for IoT applications where it is necessary to protect user identification. In the IoT with its diverse devices, safety is maintained over untrusted parties, which is desirable. But the computationally demanding and time-consuming nature of mining as well as the scaling problems that appear as the network's nodes increase in size must be addressed. The underlying protocols also generate a lot of overhead traffic, which may not be acceptable for some IoT devices with limited bandwidth. The article describes a blockchain-based architecture for the Internet of Things (IoT) that provides lightweight, decentralized security and privacy while maintaining the advantages of blockchain.

## Block-based IoT Architecture

For the architecture, a smart home setting is considered where an user (Alice) incorporates her home with a number of IOT devices (thermostat, smart bulbs, IP camera, other sensors). It consists of 3 network sections:

### Smart home

Devices: All smart devices located in the home like router, sensors, cameras etc.

Local BC & Storage: To keep (IoT) devices secure and private, a blockchain-based local record-keeping system, that is controlled by devices like a smart hub or home computer. Contrary to how Bitcoin operates, this blockchain is controlled by the device owner and has limitations on who can access it. It is simpler since transactions are grouped and recorded in blocks rather than using challenging logic puzzles. The blockchain owner inserts a pointer to the previous blocks and duplicates its access restrictions into the new block. Also, devices will communicate with one another using a secret key created using generalized Diffie-Hellman mathematics. Also, a local storage can be used to store data. Figure 1 shows the Architecture.

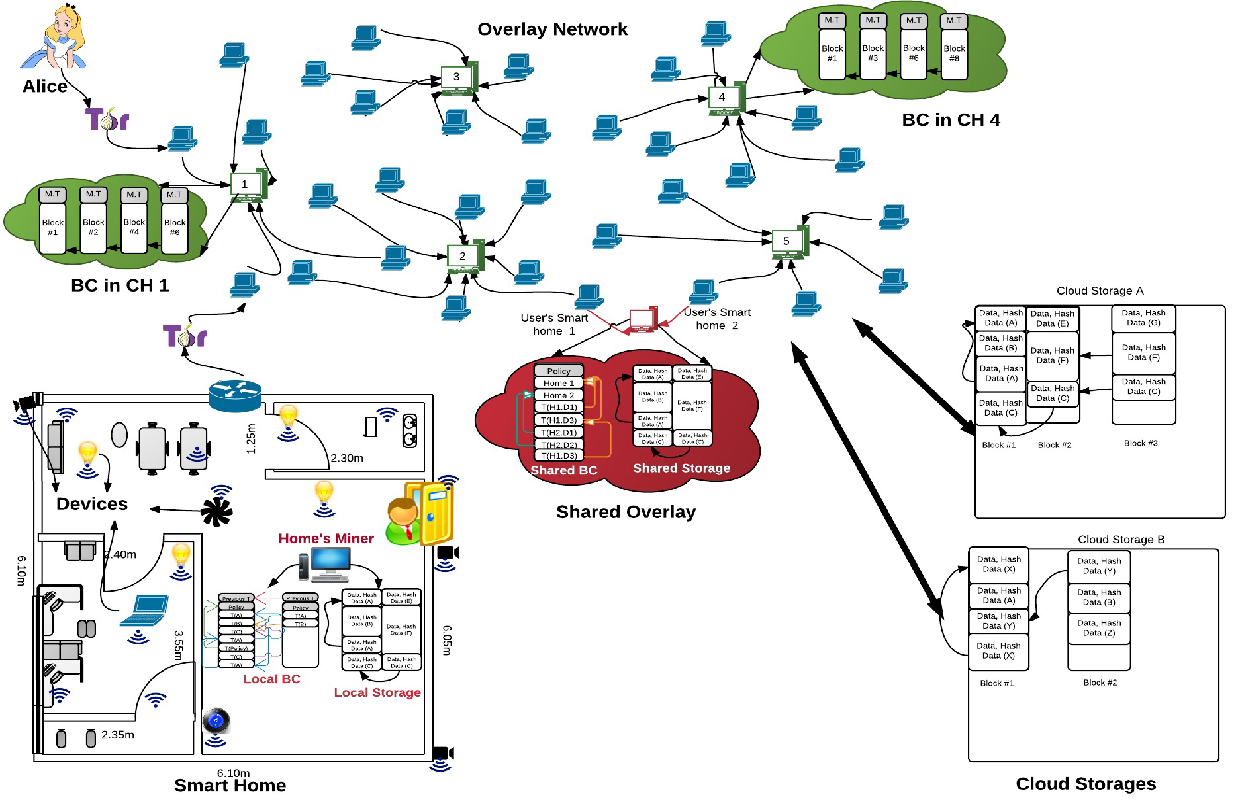


Figure 7

### Overlay Network

The overlay network is made up of a collection of networked nodes, including smart home miners, high-resource gadgets, and user devices like smartphones and desktop PCs that use Tor for further anonymity. The nodes are organized into clusters, and each cluster elects a Cluster Head (CH) to keep a list of approved requesters and requestees for data access. Based on its interaction with the parties involved in the received transaction, each CH separately chooses whether to keep a new block or delete it. This can result in various BC versions in every CH. Reduced synchronization cost may come at the expense of a longer delay in finding a specific block or transaction. If a user has multiple homes, a shared overlay consisting of high resource devices can be formed and keep track of the block number and data hash for the most recent transaction.

### Cloud Storage

Devices like Thermostats can save data in the cloud for use by external service providers to offer smart services. A hash and unique block number are used to authenticate user data that is grouped into identical blocks. Because the new block-number is encrypted using a shared key obtained from the Diffie-Hellman method, only the authentic user may access their data and chain new data to an existing record. For each device, a user can either build a unique common log or multiple distinct blocks logs containing data. This is important if the user wishes to grant a service provider access to all the data on a particular device. Data is kept in a First-In-First-Out order.

## Transaction Handling

Transaction is handled in following ways:

### Storing

Data can be stored locally, shared, or in the cloud by smart devices like thermostats. While using cloud storage, the device sends its data to a miner, who creates a special ID for the data and sends it to the storage for verification. Also, the hash of the data is sent to an overlay network to be mined in a blockchain. This is done to make sure that any modifications made to the data are accessible to everyone. In case of shared storage, there is no need for miner to send the current data's hash during a store operation as its controlled by the homeowner as well as not required to send the data hash to the overlay network. While local storage operates similarly to shared storage, all communications take place only inside the smart home. An outside miner or overlay network is not necessary. The procedures mentioned above make sure that any modifications to the data are transparent to all parties, which is crucial for maintaining trust. It ensures security by verifying permissions and ensuring that there is enough storage for the data. Figure 2 shows the mechanism for storing.

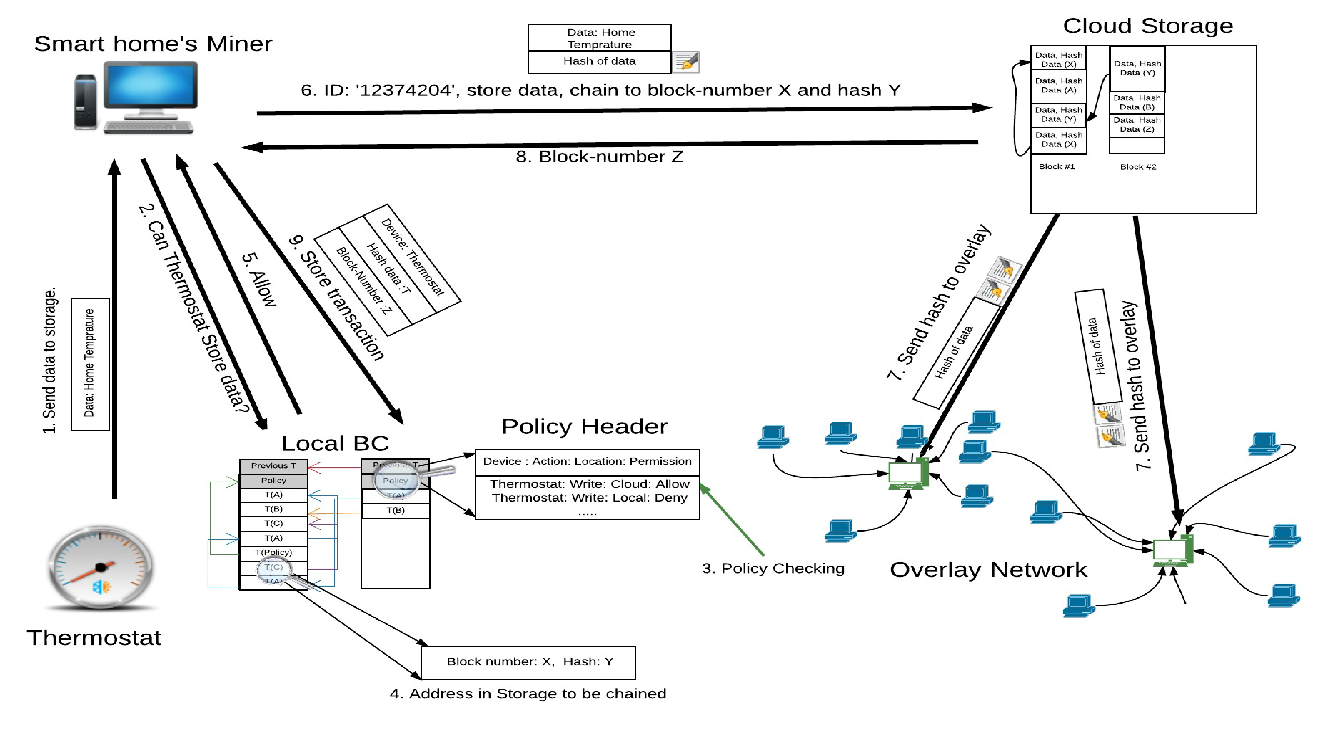


Figure 8

### Accessing and monitoring

A multisig transaction that is signed by both the SP and the miner of the smart home must be created and stored for the SP to access data that is stored on the device. The next step is to send this transaction to the user's local blockchain (BC) for verification that the SP is authorized to view the data. If yes, the miner transmits the data to the requester after encrypting it with the requester's public key. The miner has the option of encrypting the data before delivering it. Several policy levels are set for requester access to data in order to reduce network overhead. The miner sends the block-number and hash of the data stored in storage if the requester is permitted to access the whole chain of data. Otherwise, the miner uses techniques like adding noise or safe answers to deliver the least amount of data necessary to satisfy the requester's inquiry. All communication related to the transaction is recorded in the local BCs of the interested parties, and some intermediate nodes may also store the transaction for evidence and to look for illegal activity. The system tries to balance access to data for service implementation while maintaining user privacy and security. There are occasions when owners of smart homes may wish to access real-time data from their devices, such as viewing a live video feed or checking the temperature on their smart thermostat. System developers included a "monitor transaction" to make this possible. To obtain real-time data, the miner must first send a request to the requested device. For instance, if a user wants to view a real-time camera feed from a smart home security camera, the miner will make a request for that data from the camera and send it to the user. With no need to access the complete data chain or previously saved data, users can now see the status of their devices as it is right now. Figure 3 and 4 shows mechanisms for accessing and monitoring.

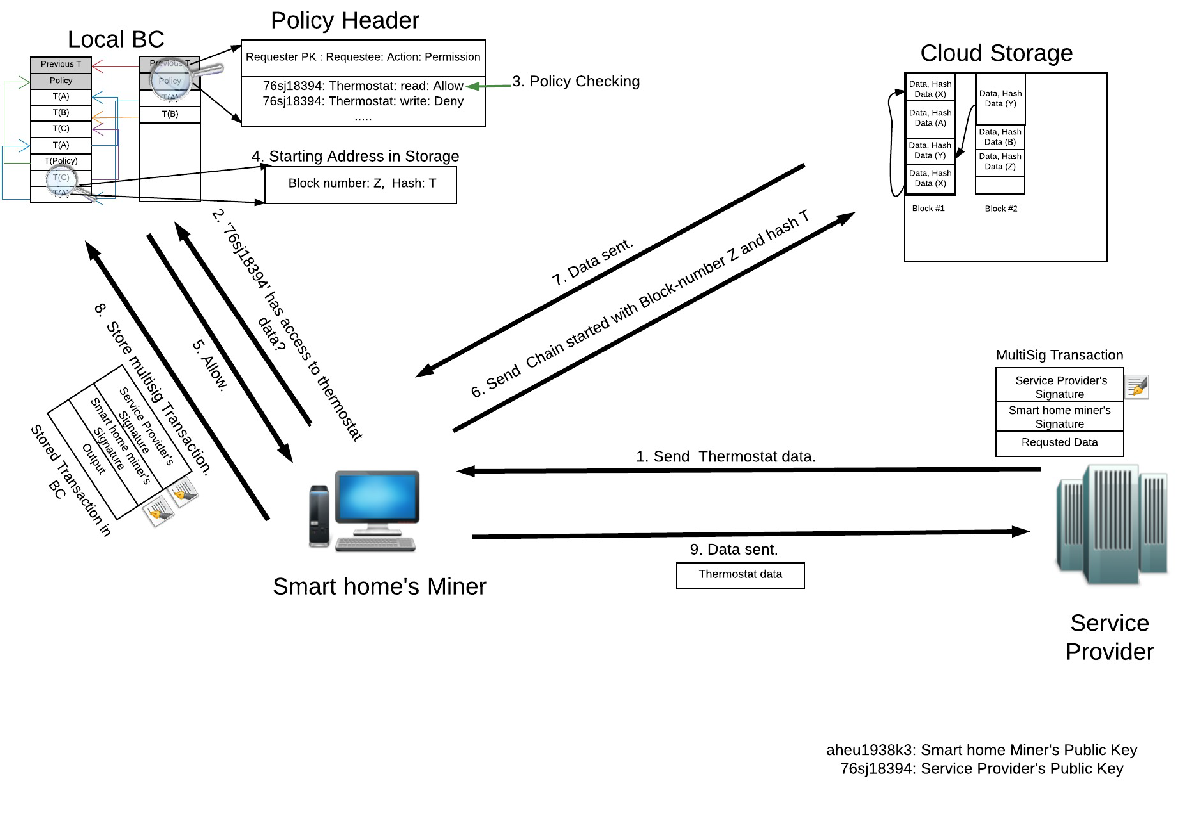


Figure 9 (Access)

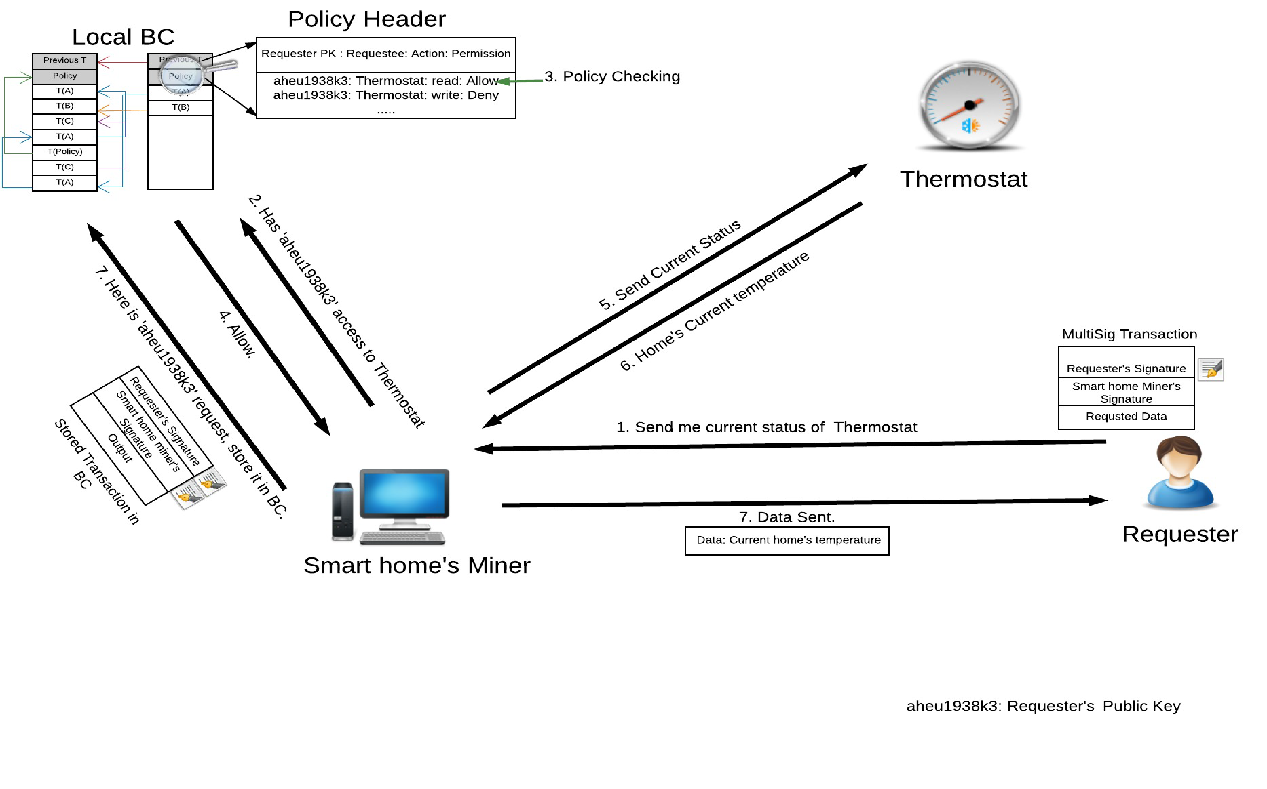


Figure 10(Monitor)

### Distributed Trust

Every Cluster Head (CH) uses the Beta Reputation System to maintain a trust rating for other CHs based on direct and indirect evidence in order to establish trust in the overlay network. Direct evidence refers to when a CH verifies a block mined by another CH (CH A has direct evidence of B if it verifies a block mined by B), while indirect evidence occurs when a CH receives a block from a different CH ( If A receives B’s block from CH C). A multisig transaction is created when a CH creates a new block and is used to assess trust. The block containing this transaction is transmitted to nearby CHs. The receiving CH tries to validate the related multisig transaction whenever a fresh block is received. It randomly verifies a portion of the transactions in the block by examining their signatures if it obtains direct confirmation from the block miner or other CHs who signed the multisig transaction. The amount of direct evidence and trustworthiness of the CHs that supply indirect evidence influence the number of validated transactions.  If it obtains direct confirmation from the block miner or other CHs who signed the multisig transaction, it randomly verifies some of the transactions in the block by examining their signatures. The amount of direct evidence and the level of trust placed in the CHs that give indirect evidence determine the number of validated transactions. A CH checks every transaction in the block if it has no direct evidence from the block creator or the people who signed it. The quantity of verified transactions and the frequency with which it has been mentioned as a trustworthy CH by other CHs both affect how trustworthy a CH is. Ultimately, this mechanism contributes to maintaining the network's high degree of security and trustworthiness by ensuring that only reliable blocks are added to the blockchain.

## Evaluation

The section assesses the overhead and performance of the suggested architecture under common security and privacy threats, assuming that adversaries can be CH, home devices, overlay network nodes, or storage. In order to validate participating nodes, the adversaries can sniff communications, discard transactions, construct false transactions, edit or delete data, link user transactions, and sign fake transactions. Accessibility, anonymity, and authentication & access control are the three main threat classifications. In the first instance, the adversary wants to keep the user from accessing her data or services. In the second instance, the adversary tries to determine the user's true identity by examining anonymous transactions and other publicly available data. In the third instance, the adversary tries to verify that she is a legitimate user in order to access data. BC architecture prevents the attackers attempts to access the data in following way:

### DOS attack prevention

In a DOS attack, the attacker aims to block access to the service or data to the authorized user. If the adversary transmits fake transactions or blocks to the overlay network or certain smart homes, the suggested architecture may be open to this attack. However, the impact of this attack is mitigated by the usage of requester and requestee PK lists in CHs. The transaction is forwarded to other CHs if neither the requester nor the requestee's PK for a multisig transaction is in either of these two lists. If a CH receives several unsuccessful access attempts from a PK, it may also block that PK and drop additional requests. By using different PKs, the attacker can still be successful in a DOS attack.

### Modification attack prevention

A malicious party can alter or remove a user's stored data through a modification attack, which jeopardizes cloud storage security. The user can, however, utilize the suggested architecture to compare the hash of the data in the cloud with the hash saved in their local blockchain in order to identify any changes to the data they have previously stored. If the user discovers a breach, they can create a transaction pointing to two transactions: the multisig transaction, which was signed by both the user and the cloud storage and contained the data's true hash, and the access transaction, which was also signed by both parties and contained an incorrect hash of the data. A number of CHs are being notified about the transaction, and they check the validity of the linked original transactions as they already have the original hash, they can detect the forged one from that comparison. When the CHs notice a difference between the two hashes, they can alert their nodes about the malicious activity by the cloud storage.

### Dropping attack prevention

In a dropping attack, the attacker takes control of one or more CHs and deletes all incoming transactions and blocks. Since the nodes in the same clusters wouldn't receive any network transactions or services because compromised CH’S are deleting all incoming requests, the suggested design makes it possible to identify such an attack. If this situation is detected, all nodes within the same cluster are informed about it, and a new CH is elected. This guarantees that even in the face of such threats, the network will continue to be secure and functional.

### Mining attack prevention

An attempt to add fake blocks to the blockchain is known as a mining attack. According to the proposed architecture, an attacker would require control over several CHs that cooperate to produce a fake block that contains a false transaction. The CHs typically verify the validity of each transaction in a block... However, in the proposed architecture, the degree of validation is based on how much the CH is trusted by the block miner or the multisig transaction signers. Thus, the CH might not validate every transaction in the block if they believe the block miner or signers. This indicates that some CH may miss to detect the fake blocks depending on the validation level but it will not go undetected by all the blocks (due to indirect evidence). If one CH detects the fake block, it can alert the others and prevent the fake block from being added to the blockchain.

### Anonymity attack prevention

An attacker tries to connect various transactions with various IDs to one genuine identity in the real world in order to break anonymity. The suggested architecture offers the sender the option of sending transactions over an overlay network to address this problem. One can send transactions through this network that are not reflected in the conventional public ledger since it functions as a layer on top of the ledger. A conventional public ledger keeps record of every transaction done in a public network which enables an attacker to track the real user. Also, each transaction that is being sent through the overlay network can have a different ID and public key (PK). This means even if someone wants to track the transactions and link it to a real user, it would be difficult for them to connect several transactions with multiple IDs to users’ true identity.

### Authentication and access control attack prevention

Threats to smart homes include attempts by hackers to access already-installed devices or add new ones without authorization. The suggested architecture prevents this because every device must be pre-defined by the user and because all transactions are logged on the local blockchain, making it simple to spot any illegal access. One possible risk is that a hacker may impersonate a genuine user to access the store and manipulate it so that the user can no longer access it. To avoid this, the architecture uses a chain of blocks, making sure that since the given block is already linked, the requester cannot attach its data to the user's data.

## IOT Conclusion

Blockchain-based IoT (Internet of Things) is growing more and more significant as the number of connected devices grows. It offers many advantages, including improved security, openness, and effectiveness.  In IoT, increased security is one of the key advantages of implementing blockchain technology. The implementation of blockchain technology will make it more difficult for hackers to control or access IoT devices, which are frequently subject to hacking attacks. Blockchain makes it simpler to detect any unwanted access or changes to the data by providing an unchanging and tamper-proof record of transactions.  Also, it provides increased transparency. Blockchain technology enables a decentralized network, allowing for the sharing and access of data by all network participants. This enables tracking and tracing the movement of data and resources, which is crucial in sectors like supply chain management and logistics. And finally, blockchain-based IoT can improve efficiency. Blockchain technology enables IoT devices to interact and deal with one another without the use of intermediaries, which can save costs and speed up processes. This is significant in sectors like finance and healthcare where quick and secure transactions are essential. In general, blockchain-based IoT has the possibility of changing how we interact with connected IOT devices and the internet by providing improved efficiency, security, and transparency.

# V. BLOCKCHAIN IN THE GAMING INDUSTRY

In the 21st century, blockchain technology is starting to grow in different industries but now it keeps its hand in the gaming industries also. Gaming is one of the largest spaces in the Entertainment

Industry. It is massive, with annual revenue of over 138 Billion USD in 2019 [9]. It also has an enormous audience, with over 2.47 billion gamers around the world by 2019 [10] It has the potential to make the gaming industry more secure and transparent as well as ownership on gaming assets and bring new monetization models. In this report we will talk about the current state of blockchain in the gaming sector, its potential benefits and some of the challenges and limitations that need to be addressed.

## Current state of blockchain in gaming:

Though the inclusion of blockchain in the gaming industry is a new concept, there are several projects ongoing to improve various fields of gaming. The first and notable example is Cryptokitties; this is a game based on blockchain where players can collect, breed and trade virtual cats where each cat is unique and different that gives the players true ownership. Ethereum is the implementation of Blockchain and permits extending its practicality with the assistance of smart contracts. Vitalik Buterin first planned the kernel of this work in Nov 2013 [11].

Another example we can give is Enjin. People can manage and build their gaming assets by using blockchain. Those assets can be sold to the Enjin marketplace that gives the game developers a new way of monetization of their gaming industries.

## Potential benefits of blockchain in gaming

For the gaming business, blockchain technology presents a number of potential advantages. Being able to offer actual ownership of in-game assets is one of the main advantages. The majority of in-game items currently belong to the game's creators, and players have no authority over them. By transferring ownership to the players through blockchain, they can sell or trade their assets as they see fit.

Enhanced security and transparency are other advantages of blockchain in the gaming industry. Since blockchain transactions are unchangeable, it cannot be theft. Because of this, it is considerably more difficult for hackers to steal in-game things or carry out other nefarious deeds. Moreover, blockchain can offer transparency in the form of accessible public ledgers, facilitating player ownership tracking and verification.

Blockchain technology has the ability to revolutionize the gaming industry in many ways. Here are some ways in which blockchain can make a significant impact:

* Real Ownership of In-Game Assets: Today, players have no authority over the majority of in-game assets, which are controlled by the game's creators. By transferring ownership to the players through blockchain, they can sell or trade their assets as they see fit. This might generate additional cash for users and result in the growth of a brand-new gaming economy. Normally we use NFT tokens like ERC-721. ERC-721 makes these tokens have a unique value and identity [12].
* More Security: By utilising distributed ledger technology and encryption, blockchain can boost the security of in-game transactions. Because of this, it is considerably more difficult for hackers to steal in-game things or carry out other nefarious deeds.
* Transparency: As blockchain transactions are permanent, they cannot be changed or eliminated. Players will find it simpler to trace and confirm the ownership of in-game assets thanks to the transparency this offers in the form of open and public ledgers.
* Alternative Monetization Features: Blockchain can make it possible for users and game producers to monetize in new ways. A blockchain-based platform called Enjin, for instance, enables game developers to build and manage in-game assets like armor, guns, and other stuff. The Enjin Marketplace offers a new opportunity for gamers to monetise their gaming experience by allowing trading and selling of these assets.
* Decentralization: Blockchain can make game development and distribution decentralized. Blockchain technology allows game makers to avoid conventional publishers and sell their products directly to users. This might encourage greater variety and creativity in the gaming sector.

As a result of its actual ownership of in-game assets, enhanced security and transparency, new monetization models, and decentralization, blockchain has the potential to have a huge impact on the gaming industry. As the technology continues to develop and mature, we should expect to see more blockchain-based games and platforms emerge in the future years.

## Different Types of Blockchain used in Gaming Industry

### Etherium

One of the most widely utilized blockchains in the gaming industry is Ethereum. Developers have been able to construct decentralized apps (dApps) for gaming that offer a variety of features including non-fungible tokens (NFTs), in-game assets, and virtual money thanks to its smart contract

capabilities and ERC-20 token specifications. The first token standard adapted by the Ethereum Blockchain is ERC-20 (Ethereum Request for Comment) which supports Fungible Tokens only [13].

The production and exchange of NFTs is one method Ethereum being used by the gaming industry. NFTs are one-of-a-kind digital assets that are kept on the Ethereum blockchain and may stand in for anything from digital art to in-game stuff. In numerous markets, players may buy, sell, and trade NFTs, giving them the ability to actually own their in-game possessions.

Ethereum can also be used to power decentralized autonomous groups in the gaming industry (DAOs). These are digital companies that run on the Ethereum blockchain utilizing smart contracts, and they may be used by the game industry to simplify community governance and decision-making.

Ethereum may also be used to handle in-game micropayments and other transactions. It is the best option for developers wishing to incorporate blockchain technology into their gaming apps because of its quick transaction processing times and affordable transaction costs.

ERC-1155 is the new final token standard on the Ethereum Blockchain[14]. It supports the characteristics of ERC-20 (Fungible) and

ERC-721, making it a worldwide standard (Non-Fungible). Because of its ability to support many tokens in a single trade, it makes it possible for gaming elements to have real-world value. With the launch of ERC1155, trading and token production are now easier. ERC 1155 permits both the conversion of current tokens and the creation of new tokens from them. Although gaming is the sole subject of this article, ERC-1155 has applications in a number of other fields, such as documentation and artwork.

Overall, using Ethereum in the gaming industry has a number of advantages, including increased ownership and control over in-game assets, enhanced security and transparency, and new business options for creators.

### TRON

Another well-known blockchain technology in the gaming sector, TRON, is utilized for decentralized gaming apps (dApps). TRON is the perfect platform for gaming apps that need quick and efficient transactions since it offers high throughput, low latency, and cheap transaction costs. The development of blockchain-based gaming systems that let users to earn cryptocurrency incentives by playing games is one method TRON is used

to the gaming industry. The native cryptocurrency of TRON, TRX, is frequently used by these sites to pay for in-game items and incentives.

Similar to how Ethereum is utilized in the gaming industry, TRON may also be used to develop NFTs. TRC-721 tokens, which are singular and indivisible digital assets that may be used to represent in-game objects, characters, or other virtual assets, are used to represent NFTs on the TRON platform. TRON may also be used to build DAOs, or decentralized autonomous organizations, that are tailored for gaming communities. These DAOs can help with community decision-making, governance, and incentive distribution.

Nevertheless, using TRON in gaming has advantages including quick and seamless transactions, affordable costs, and the chance to receive crypto currency prizes for playing games. Moreover, it gives developers the chance to use blockchain technology to produce fresh gaming experiences and business models.

### EOS

Another blockchain technology utilized in the gaming sector is EOS, which enables developers to build decentralized apps (dApps) and provide gamers specialized gaming experiences. EOS is a desirable option for gaming applications due to its high throughput, quick transaction processing times, and cheap transaction costs.

The development of blockchain-based gaming platforms that let users earn cryptocurrency incentives by playing games is one method EOS is applied to the gaming industry. EOSIO, the native money of EOS, is frequently used on these platforms to pay for in-game items and incentives. Moreover, non-fungible tokens (NFTs), which stand in for exclusive in-game assets or goods, may be made using EOS. Players may really own and control their in-game assets thanks to the ability to buy, sell, and trade NFTs on a variety of online markets.

Decentralized autonomous organizations (DAOs), which are intended to promote community governance and decision-making, are another way that EOS is used by the gaming industry. These DAOs may be used to manage in-game resources, develop fresh game features, and compensate participants. EOS may also be used to develop in-game markets, which let players exchange in-game goods and assets directly with one another rather than going via middlemen or external marketplaces.

Overall, using EOS in gaming has advantages including quick and seamless transactions, affordable costs, and the chance to receive crypto currency prizes for playing games. Moreover, it gives developers the chance to use blockchain technology to build fresh gaming experiences and business structures.

## Challenges and Limitations

Before blockchain can be widely used in the gaming business, there are a number of obstacles and restrictions that need to be overcome in addition to the potential advantages. Scalability is one of the main obstacles. Currently, the majority of blockchain systems have restricted capacity, which means they can only process a specific number of transactions per second. For games with a huge player base or many transactions, this might be a serious restriction.

User adoption presents another difficulty. Blockchain is still a young technology, thus it might not be well known to many players. Also, some players may be turned off by the complexity of using the blockchain to acquire and sell in-game goods compared to more conventional means.

## Gaming Conclusion

In conclusion, blockchain technology has the potential to revolutionize the gaming sector by enabling actual in-game asset ownership, greater security and transparency. Before blockchain is extensively used in the gaming business, there are a few obstacles and restrictions that must be overcome. In the upcoming years, we may anticipate the emergence of additional blockchain-based platforms and games thanks to ongoing innovation and development.

# VI. BLOCKCHAIN AND NFTs

Non-Fungible Tokens (NFTs) are a kind of digital asset that has seen significant growth in popularity in recent years. Although NFTs themselves are not novel, the innovations in blockchain technology that have allowed for their creation, verification, and transfer of ownership make them a practical reality. Non-fungible tokens (NFTs) are non-transferable digital assets that may be used as evidence of ownership or originality. Each NFT is one-of-a-kind and cannot be duplicated, unlike fungible cryptocurrencies like Bitcoin that can be traded for other cryptocurrencies or fiat money. Because of their rarity and genuineness, NFTs are highly sought after by collectors and enthusiasts. Blockchains, a kind of distributed ledger technology that ensures the integrity and transparency of all transactions, are used to generate NFTs. The blockchain records a unique identification for each NFT, allowing buyers and sellers to confirm the digital asset's ownership and legitimacy. Once an NFT is produced, its originator and any future buyers or sellers will always be known, and the NFT's ownership will always be verifiable.

Digital art is one of the most well-known applications for NFTs. By using NFTs, creators of digital works may present and market them as original works of art, rather than as readily replicable digital files. This has provided artists with whole new avenues for making money off their digital works and sharing them with people all over the world. In addition to their application in the industries, NFTs have found their way into the gaming, music, and sports industries. In the gaming industry, NFTs may stand in for special objects or characters, while in the music industry, they might signify ownership of a certain song or album. To a sports fan, a non-fungible token (NFT) might be a collectable object associated with a certain player or a share of a memorable event during a game.

The value of NFTs has skyrocketed at online auctions in recent years, with some fetching millions of dollars. On the contrary, NFTs are susceptible to security vulnerabilities that may undermine their integrity and value, just like any other digital asset. The process of manufacturing and transporting NFTs consumes a lot of energy and may contribute to carbon emissions, which also raises worries about the technology's effect on the environment.

## NFT Mechanism

NFTs, or Non-Fungible Tokens, work by using blockchain technology to create a unique and verifiable digital asset that represents ownership or proof of authenticity of a particular item or piece of content. NFTs are distinguished by the following distinct qualities [15]:

Each newly created coin is assigned a one-of-a-kind identification that is inextricably bound to a specific Ethereum address.

They cannot be used in place of other tokens on a one-to-one basis directly. For instance, 1 ETH and another ETH are equivalent to one another in every way. When it comes to NFTs, this is not the case.

Each token has a corresponding owner, and it is simple to confirm this information.

They exist on Ethereum and may be purchased and traded on any non-fungible token (NFT) market that is based on Ethereum.

To break down how NFTs function in layman's terms [15]:

Digital works of art and music start with their first creation by their respective creators. The designer then uses NFT-specific software to give each of these items a unique code that is recorded on a distributed ledger called a blockchain. The blockchain serves as a distributed ledger to verify the legitimacy of the NFT and record the transactions that have taken place with it. This offers a safe method of establishing ownership and validity of the NFT and makes it impossible for a counterfeit version to be created. Transferring ownership of an NFT is accomplished by a blockchain update after its sale or exchange. Creating a clear and easily accessible ownership record. When an NFT is sold or exchanged, the blockchain is updated to reflect the new owner's information. As a result, a fresh public ownership record is generated that can be validated by anybody with access to the blockchain.

Diagram

Description automatically generated

Figure 11: How blockchain mechanism used for NFT [16]

## Blockchain in NFT

NFTs function by producing a one-of-a-kind digital asset that can be verified and used as evidence of ownership or originality of a certain object or piece of information. In order to verify ownership and transfer the NFT between buyers and sellers, blockchain technology is used.

The usage of blockchain technology in NFTs comes with several advantages, including the following [17]:

### Security

The use of blockchain technology helps to guarantee that non-fiat currencies are safe and cannot be altered in any way. Because of the decentralised structure of the blockchain, it is very difficult to break into or manipulate, which ensures that the NFTs will continue to be valuable and real.

### Transparency

The use of blockchain technology guarantees that the ownership of the NFT is open to public scrutiny and can be independently verified. Because of this, a public record of ownership is generated, which can be confirmed by anybody who has access to the blockchain. As a result, it is far more difficult to argue about who really owns anything.

### Accessibility

The use of blockchain technology makes it possible for NFTs to be accessed by anybody who has a computer and an internet connection. This paves the way for new options for producers, artists, and collectors to interact with digital information in a manner that is deeper and more genuine.

### Flexibility

The usage of blockchain technology makes it possible for NFTs to be quickly moved and sold between buyers and sellers. This provides a degree of flexibility. This results in the establishment of a liquid market for NFTs, which makes it possible for producers and artists to establish new income streams.

To summarize, blockchain technology is an important component of NFTs because it offers a safe and open system for the generation, verification, and transfer of ownership of one-of-a-kind digital assets. Since the use of blockchain technology assures that NFTs are safe, transparent, accessible, and adaptable, it paves the way for new options for creators, artists, and collectors to interact with digital information in a manner that is more meaningful and genuine.

## NFT Applications

Blockchain technology's NFTs are revolutionary. NFTs have many blockchain applications:

* Art and Collectibles: NFTs are often used in art and collectibles. Artists may sell one-of-a-kind NFTs to customers. Each NFT depicts a distinct sports card or trading card.[18]
* Gaming: NFTs are used to produce uncommon in-game products that can be sold on the blockchain. These things may be owned and traded, giving game producers a new money source and giving gamers a more immersive and engaging gaming experience.[18]
* Music: NFTs are used to make unique digital albums, concert tickets, and other mementos. NFTs provide fans evidence of ownership and authenticity, as well as a fandom-themed treasure.[18]
* Real estate: NFTs symbolize property ownership. Each NFT represents a unique property and proves ownership. This streamlines and clarifies real estate transactions.[19]
* Identification Verification: NFTs verify digital identities. Secure login authentication, financial transaction identification verification, and other identity verification applications may leverage this.[18]
* Charity Fundraising: Each NFT donates to a charity. The charity may sell or trade the NFT to generate income and publicity.[20]
* Intellectual property: NFTs safeguard intellectual property. NFTs prove ownership and validity for creators. This prevents copyright infringement.[19]

Finally, NFTs are used in the fields of credentialing, gambling, music, royalties, generating money for charities, and more. NFTs allow users to create, own, and exchange one-of-a-kind digital assets, which opens the door to additional revenue sources and a more real and interactive user experience. With blockchain technology, NFTs are made more secure, transparent, and tamper-proof, which alters the nature of digital ownership and value.

## Key Challenges of NFT [21]

“A review of the key challenges of non-fungible tokens” [21] is a paper that examines the difficulties inherent to the Non-Fungible Tokens (NFTs) industry at large.The purpose of this paper is to provide an answer to this issue so that researchers of the future may better understand the obstacles that must be overcome before NFTs can be widely used. The current investigation was carried out between January 24th and April 23rd, 2022, according to the procedures detailed in the preparation phase. A total of 317 items were found in the first search. After going through the seven primary issues mentioned below, including review phases, quality evaluation criteria, the suggested methodology, and the classification system, just 42 articles remained.

### Usability Challenges

Initially due to the usage of smart contracts in the processing of NFT transactions to ensure their veracity and transparency, confirmation times may increase. A crucial challenge for NFTs is the price of gas, which may increase dramatically before and after the minting process and data upload to the blockchain.

### Privacy Issues

The privacy and anonymity of NFT transactions are reportedly dependent on the underlying Ethereum platform, which provides a level of pseudo anonymity. In addition, the inability to access NFT data limits its value and prevents it from being utilised in other settings.

### Governance Consideration

While working with NFTs, it is important to keep several different elements of governance in mind. Lack of government regulation of NFTs means that those involved in creating, selling, buying, or investing in them have very little legal safeguards. In addition, property taxation related problems, goods associated with intellectual property are regarded as taxable assets under the present regulations.

### NFT Security Issues

The use of blockchain technology enables several different security methods, which secure non-fungible tokens.

* Spoofing: Blockchain secures NFT transactions using public-key cryptography. Sender's private key signs and public key verifies each transaction. This avoids spoofing by limiting transaction initiation to the proper owner. When an NFT is moved from one wallet to another, the blockchain records the transaction and updates NFT ownership. This prevents NFT spoofing and duplication.
* Tampering: Blockchain stores transactions on a decentralized ledger. Blockchain transactions are permanent. This protects NFT data from manipulation. A blockchain-minted NFT's metadata cannot be changed.
* Repudiation: Blockchain technology keeps transactions indestructible. This prevents a statement's creator from disputing it. When an NFT is sold, the blockchain records the transaction and transfers ownership. This guarantees that the former owner cannot dispute selling the NFT.
* Information disclosure: Cryptography secures NFT transactions and protects user privacy in blockchain technology. Cryptographic algorithms encrypt and verify each transaction, preventing unwanted disclosure. The receiver can only decode an NFT transaction. This prevents information disclosure.

### Extensibility Issues

This aspect has two parts; first, if the system is robust enough to communicate with other ecosystems; second, whether an NFT system can supply itself with updates when the present version becomes obsolete. Nevertheless, because of the lack of NFT interoperability, users are limited to transacting in NFTs inside their chosen platform's ecosystem or network. Next, there are updatable NFTs. Blockchains may upgrade their protocols through soft forks (small modifications that are backwards-compatible) and hard forks (substantial changes that break compatibility with older versions of the system) (major changes that may cause conflicts with previous protocols).

### Environmental Factors

Despite research showing that crypto harms the environment, NFTs and comparable technologies are drawing individuals into the industry. Some newer blockchains, such Polygon and Hedera, are carbon neutral, but Ethereum, which supports NFTs, is expected to require a lot of energy and harm the environment. Blockchain mining's proof-of-work algorithm uses a lot of energy, making environmental sustainability a major issue for NFTs. After finding NFT requires significant energy use, French digital artist Joanie Lemercier canceled his project. Next-generation verification consensus mechanisms like proof-of-stake are replacing miners with validators that possess more bitcoin assets, cutting power use. Validators may be rewarded for offering their tokens as collateral.

### Intellectual Property Issue

Intellectual property is a major concern among the risks and challenges associated with NFT. Confirming the seller's authorization to sell the NFTs in issue is crucial before conducting any kind of transaction. Non-monetary transfers (NFTs) of pictures or copies have occurred, which might lead to intellectual property (IP) difficulties. An NFT owner's rights and obligations are spelled out in fine detail in the integrated smart contract data. Although NFT applications have the potential to be lucrative, there are several challenges that must be surmounted before that can happen. Rising NFT trading volume is indicative of the asset class's growing appeal and bright future. Since there is no uniform law to regulate NFT trading, and because intellectual property rights are not adequately protected, there is a risk that consumers may be wary of and slow to embrace this technology. Addressing these problems via regulation is necessary for building user trust and promoting widespread adoption of NFTs.

In the blockchain industry, the NFT is a newfangled innovation that is quickly gaining traction. There is a dearth of research material on NFTs since they are relatively new technologies. Thus, this review article completes the literature gap by offering a comprehensive overview of both current and future difficulties.

## Mitigation of NFT Key Issues

The risks associated with Non-Fungible Tokens (NFTs) may be mitigated in several ways, and developers, investors, and traders can utilise these strategies.

* To protect your NFTs, always use a private key to access your digital wallet; never store your NFTs using a public key. Popular NFT wallets include MetaMask and MyEtherWallet.[23]
* Developers make NFTs with the help of blockchain and smart contracts. Developers should follow standard procedures while building smart contracts to guarantee the legality and authenticity of their agreements. It is also suggested that the contract code be tested and audited thoroughly to find and correct any security flaws.[24]
* In most cases, decentralized markets are safer against hacking than centralized exchanges. Decentralized markets like OpenSea and Rarible use blockchain technology to provide a safer alternative to controlled markets.[23]
* It is possible to increase the safety of digital wallets by using multi-factor authentication, which requires many authentication steps before providing access. Biometric authentication, physical keys, and one-time passcodes texted to a mobile device are all examples of this.[24]
* Standardization and regulation of the NFT market are important to safeguard both buyers and sellers, which would improve the market's appeal. As part of a larger industry-wide effort to avoid fraud and enhance transparency, legal frameworks and standardized methods to smart contract creation and associated information may be implemented.[24]

In conclusion, it is possible that the dangers associated with NFTs may be mitigated using safe wallets, best practices in smart contract design, decentralized markets, multi-factor authentication, and standardization and regulation of the market. With these protections in place, users, merchants, and investors may feel more comfortable transacting in NFTs, which might hasten their wider adoption as a disruptive technology in the digital economy.

## Future of NFT

Non-Fungible Tokens (NFTs) are a revolutionary concept that has the potential to disrupt several industries. Although still in their infancy, NFTs have already facilitated the birth of new marketplaces and the spread of innovative practices for the management, distribution, manipulation, and archiving of digital data. NFT development has moved through heritage phases and into exploration, with a persistent drive for exploitation, even if we are still in the early adoption stage. NFTs have been reported to generate disruption across a wide range of markets, including the fine arts, sports, law, escrow, tickets, digital collectibles, gaming, and crypto-technical sectors.

Researchers in the paper "Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity"[24] also predicted that novel products like NFT Bonds and augmented and virtual reality technology would cause disruptions in the real estate, automotive, and financial markets in the near future.

In addition, the incorporation of NFTs into non-digital, tangible consumer things improves the owner's and the community's interaction with the real object and its digital counterpart. Bags, jewelry, apparel, event tickets, and shoes are just some of the items that have NFTs implanted inside them. Nike's Cryptokicks patent is innovative since it employs NFT coins to verify the genuineness of shoes. The NFTs have several potential applications, including but not limited to retail, trading, gaming, and user interaction. The use of NFTs is also on the rise as a means for companies to provide discounts, subscriptions, and other perks to their customers. They can make it possible to provide more dedicated fans access to more specialized material. The band Kings of Leon, for instance, tied NFTs with the release of their album by giving the highest bidders a golden ticket NFT that granted them access to VIP amenities including front-row seats, backstage passes, and a moving record cover.

In conclusion, the future of the technology behind non-fungible token blockchains seems promising, with the possibility of increasing acceptance, interoperability, scalability, and sustainability, as well as the introduction of new use cases. As the technology advances further, it is expected that additional applications and possibilities will become available. They will contribute to the development of a digital economy that is safer, more transparent, and less centralized.

# VII. BLOCKCHAIN IN BANKING

Banking is crucial to an economy's smooth operation. Credit and other financial services, which are necessary for businesses to grow and invest in new projects, are accessible through banking. In turn, this encourages economic expansion and leads to job creation. On the other hand, individuals and businesses can store their money in a secure environment at a bank. This ensures that they can access their funds whenever they need them while also preventing the loss or theft of their savings. Additionally, this system makes it easier for individuals and businesses to send and receive money, which is crucial to the economy's operation. Transacting would be much more time-consuming and difficult without banks. In addition, banks support government operations by providing a variety of financial services, such as managing government accounts, processing tax payments, and facilitating loans to fund government projects. These services, which help individuals and businesses plan for the future and make informed financial decisions, include retirement planning and investment advice. Overall, the banking sector is pervasive and significant, and it has a significant impact on our day-to-day lives because it makes it possible for us to manage our finances and carry out transactions. In order to make purchases and withdraw cash, we make use of banking services like debit and credit cards. Additionally, we use mobile and online banking services to access our accounts and carry out online and mobile transactions.

## Traditional Banking System

The banking system that existed prior to the rise of digital banking is referred to as the traditional banking system. It has served as the foundation of the global financial system and continues to play a crucial role in assisting individuals, businesses, and the economy as a whole. Traditional banking still plays a crucial role in the global financial landscape, despite some criticisms and difficulties. Traditional banking systems involve carrying out transactions and other banking activities through the use of actual branches and face-to-face interactions between customers and bank employees [26][28] [29].

Diagram

Description automatically generated

Fig. 12: Traditional Banking System [26] [30]

In the current banking framework, people and organizations can visit a physical branch to open an account and store cash. After that, the bank will keep this money and use it to make loans to other customers, bringing in interest for the bank. Additionally, customers can request a withdrawal by visiting the branch and withdrawing funds from their accounts. In addition to these fundamental services, banks can offer a wide range of additional financial services, including facilitating payments and transactions, issuing credit and debit cards, and offering investment and wealth management products. All of a customer's financial transactions are recorded and tracked by banks using a centralized database to guarantee the system's security and integrity. The bank keeps a close eye on and manages this database, which is used to keep track of all transactions and prevent fraud. In addition, banks use a variety of security measures to safeguard the database and prevent unauthorized access, such as authentication and encryption. Banks play a crucial role in the economy as a whole because they provide a stable and secure environment for financial transactions. This is in addition to providing customers with financial services. They help to match people who have extra money with people who need money to buy or invest. They also act as a link between lenders and borrowers. This facilitates the movement of capital throughout the economy and may support economic expansion. So, the traditional banking system is characterized by the use of cash as the primary mode of payment, face-to-face interactions, and physical branches. It is possible to be inconvenient and costly for both banks and customers, despite the fact that it has some advantages in terms of developing personal relationships with customers.

## Key Challenges of Traditional Banking System

* **Inefficiency:** When it comes to moving money between accounts and processing transactions, traditional banking systems can be slow and cumbersome. Customers may experience delays and inconvenience as a result, and banks may incur higher costs as a result. Furthermore, transactions can take longer time to complete due to the manual processes used in traditional banking systems. Customers who need immediate access to their funds or payments may find this frustrating.
* **Limited Accessibility:** Customers of traditional banking systems frequently have to go to a physical branch to open an account or do other transactions. This can be awkward for clients, particularly for the people who live in remote or underserved regions. On the other hand, most of the time, physical branches of traditional banks are open during specific business hours. Customers who work during those hours or live in remote areas may find it challenging to access banking services as a result of this specific business hour frame. They might have to travel a long distance to visit a branch or stand in long lines.
* **Lack of Transparency:** Customers have a difficult time understanding how their money is being used and what fees and charges they are paying because traditional banking systems may not be transparent enough. Customers may find it difficult to make informed financial decisions as a result of this lack of transparency.
* **Centralization:** A small number of large financial institutions typically have control over traditional banking systems, making them susceptible to failure or collapse in the event of a crisis. These institutions may also gain significant economic power and influence as a result of this centralization.
* **Security Deficiency:** Traditional banking systems depend on central databases to record and track monetary exchanges, which can be helpless against hacking and different types of cyber-attack. Customers' financial and personal information may be at risk as a result of this. On the other hand, because of dealing with physical cash and paper-based transactions, traditional banking systems are more susceptible to security breaches like theft or fraud. This can also be a main issue for clients who need to safeguard their cash and individual data.
* **Higher Costs:** Due to the necessity of operating physical branches and employing staff to manage them, traditional banks have higher operating costs than digital banks. Customers are frequently subjected to lower interest rates and higher fees as a result of these expenses.
* **Lack of Innovation:** Traditional banks may be at a disadvantage because they have been slow to adopt new technologies and innovations with proper security. Their capacity to offer new and improved services to customers may be limited as a result of this.

So, the traditional banking system faces several challenges that can impact its ability to provide efficient and effective services to customers. As a result, banks are increasingly looking for ways to adapt to changing customer needs and preferences, including through the adoption of blockchain technologies [27][28][29].

## How can the Banking Sector Benefit from Blockchain Technology?

Blockchain technology can possibly reform the banking area by offering secure and straightforward exchanges, eliminating the need for intermediaries, reducing costs, and further improving productivity. So, by reducing the need for intermediaries and enhancing the efficiency and transparency of financial transactions, blockchain technology has the potential to have a significant impact on the banking sector. It is a decentralized and distributed digital ledger that can safely and effectively record transactions across a computer network without requiring a centralized authority. Because of this, the banking industry, which has traditionally relied on intermediaries to facilitate transactions, could benefit from its use. Without the need for middlemen, secure transactions between parties are made possible by blockchain technology. Each transaction is authenticated, validated, and recorded on the blockchain ledger using cryptography. This ensures the security of financial transactions by making it virtually impossible to alter the transaction data. Additionally, transactions are completely transparent due to blockchain technology. The transaction data on the blockchain ledger is accessible to all parties involved in the transaction. Because any suspicious activity can be easily identified and traced back to the source, this makes it possible for banks to lessen the likelihood of fraudulent transactions occurring. Also, blockchain technology has the potential to significantly cut down on the costs of conventional banking transactions. It streamlines banking operations and increases efficiency by eliminating the need for intermediaries like clearinghouses, custodians, and settlement agents. This can save banks billions of dollars annually. Real-time transaction processing eliminates the need for lengthy settlement periods. This may assist banks in lowering operational expenses and enhancing customer service. Furthermore, by making transactions faster, safer, and more transparent, blockchain technology can enhance the customer experience. With the ability to view account information and track transactions in real time from any location, customers can have greater control over their finances.

Diagram

Description automatically generated

Fig. 13: Blockchain in Banking emphasizing Distributed Ledger Technology (DLT) [30]

On the other hand, in the current banking system, due to the necessity of intermediaries and the possibility of fraud, the settlement of transactions can be slow and costly. So, payments and other financial instruments can be settled more quickly and safely with the help of blockchain technology, reducing the need for middlemen and the risk of fraud. As a result, financial transactions can become more affordable for both individuals and businesses. The development of brand-new financial services and products is another potential area where blockchain technology can be utilized. Blockchain technology enables the development of new types of financial instruments that are not dependent on traditional intermediaries, such as banks and other financial institutions as it is decentralized and distributed. In the financial sector, this may present new opportunities for creativity and competition, which may result in the creation of new goods and services to the advantage of both businesses and customers.

## How does a banking system with Blockchain Technology work?

A banking system with blockchain technology works by utilizing the decentralized, transparent, and immutable nature of the blockchain record to facilitate secure, productive, and cost-effective transactions. Also, by making financial transactions faster, safer, and more transparent, blockchain technology has the potential to transform the traditional banking system. On a blockchain based banking system, customers are able to open accounts, deposit and withdraw money, and carry out other financial transactions easily. Here is a straightforward illustration of how a banking system based on the blockchain might function [27][28][29]

* **Making a Blockchain Network**: First, banks need to set up a private blockchain network that only authorized parties can access. They can use existing blockchain platforms like Hyperledger Fabric or Ethereum or create their own.
* **Digital wallet creation:** A customer creates a new digital wallet and private key for a new account on the blockchain. So, the digital wallets that are protected by private keys are made available to customers. Their digital assets, such as tokens or cryptocurrencies, are stored in these wallets.
* **Initiating Transactions:** By sending a digital transaction to the blockchain, the customer deposits money into their account, which is checked and recorded on the ledger. Also, the customer can then use their digital wallet to send and receive payments and engage in other blockchain-based transactions. So, in detail, a customer's transaction is broadcasted to the network and validated by consensus algorithms by multiple nodes. The transaction is possibly approved in the event that it meets specific models, for example, having adequate assets and meeting regulatory requirements.

A picture containing diagram

Description automatically generated

Fig. 14: Banking scenario based on Blockchain [29].

* **Recording Transactions:** When the transaction is approved, it is recorded on the blockchain ledger in a block that is cryptographically connected to the past block. This makes an immutable record of the transaction that is sealed and can be accessed by authorized parties. So, multiple computers on the network verify the accuracy and security of the transactions before they are recorded on the ledger.
* **Settlement:** On the blockchain network, settlement is carried out immediately. There are no middlemen involved in the transfer of funds from the buyer's digital wallet to the seller's digital wallet and, by using the blockchain ledger, the customer can access their account balance and transaction history at any time.
* **Regulation and compliance:** Banks must ensure that they adhere to regulations like Know Your Customer (KYC) and Anti-Money Laundering (AML). They can automate compliance checks and ensure that all transactions comply with regulatory standards by using smart contracts.

So, a method for facilitating transactions that is secure, transparent, and effective is provided by a banking system that uses blockchain technology. By eliminating intermediaries, reducing costs, and improving efficiency, banks can offer better types of services to their clients while additionally reducing risks and increasing benefits [26].

Blockchain-based banking relies heavily on Central Authority. It will establish the participants, authorization of nodes, types of networks, creation and management of smart contracts, supervision of financial institutions, and other aspects of the network as a whole. Because it provides access to multiple organizations and institutions through a single blockchain network, consortium blockchain is the most popular choice in the banking industry. Through the common blockchain network, one financial institution can access the records and customer information of another financial institution. Customers' credit histories can be checked in the same way by creditors. Every blockchain node has a single, replicated copy of the entire database, making the system stable, secure, transparent, and dependable all at the same time.

# VIII. SECURITY IMPACT OF BLOCKCHAIN TECHNOLOGY WITH EXISTING SYSTEMS

The following are some typical methods of attack that would not work on a blockchain network.

* **Man-in-the-middle attacks**: An attacker could attempt to intercept and alter communications between two parties in a traditional network in order to gain access to sensitive information or disrupt the network. Digital signatures and other cryptographic methods make it difficult for an attacker to carry out this kind of attack unnoticed in a blockchain-based network.
* **Central Server Hacking**: An attacker could attempt to compromise the central server in a traditional network in order to access sensitive data or disrupt the network. Since there is no central server in a blockchain-based network, this kind of attack would not be possible.
* **DDoS attacks**: An attack strategy known as a distributed denial of service (DDoS) attack is frequently used by attackers to flood a network with traffic and make it crash or unavailable. DDoS attacks are highly resistant to a distributed and decentralized nature of a blockchain-based network.
* **Race condition attacks**: An attacker could attempt to take advantage of concurrency vulnerabilities in a conventional network in order to access sensitive data or disrupt the network. Consensus mechanisms can help prevent race condition attacks in a blockchain-based network.
* **Malicious hubs**: In order to gain access to sensitive data or disrupt the network, an attacker might attempt to compromise individual nodes in a conventional network. Cryptographic methods and consensus mechanisms make it difficult for an attacker to compromise a node in a blockchain-based network without being noticed.
* **Sybil attacks**: An attacker could attempt to make different fake identities in order to gain disproportionate influence or control over the network. Using proof-of-work or proof-of-stake mechanisms in a blockchain-based network can make it hard for an attacker to create fake identities without being noticed.
* **Replay attacks**: An attacker could try to capture and replay a valid transaction in a traditional network in order to access sensitive information or disrupt the network. Replay attacks can be prevented in a blockchain-based network by employing sequence numbers and other mechanisms.
* **Front-running attacks**: By changing the request for exchanges or accessing special data, an attacker could attempt to gain an unjustifiable advantage in a conventional organization. In a blockchain-based network, transparent and accessible ledgers can make it hard for an attacker to launch front-running attacks without being noticed.
* **Routing attacks**: An attacker could attempt to disrupt the flow of information in a traditional network by compromising or disrupting the routing infrastructure of the network. The distributed and decentralized nature of a blockchain-based network can make it more resilient to routing attacks.

# VIIII. CONCLUSION

In conclusion, through our exploration of many fields in which blockchain technology was researched to be implemented and indeed implemented, we have seen a great ubiquitous interest in this technology and how it can be integrated usefully as soon as possible. Military applications were found to be great to prevent a central point of failure issue as well as error tracing to find out the source of a problem. IOT applications greatly aid security for those devices as they are usually the targets for botnets, this is accomplished with tamper proof ledgers found on those devices, this also aids in production efficiency as well. Gaming applications can give players real ownership to in-game items as well as greatly increase security and transparency when it comes to online games. NFTs are essentially based on the blockchain and it has advantages in its scalability, exclusivity, interoperability, and many other advantages, it enables artists to take ownership of their pieces and make a good amount of money on top of it, thus encouraging creativity. Finally, Blockchain in Banking is probably the application blockchain was built on, it offers secure traceable transactions to prevent crimes such as wire fraud, it also helps eliminate unnecessary intermediaries thus speeding up the process of transfers; even with this speed blockchain is great for verification and security through its cryptographic protocols so the elimination of those intermediaries is not a problem.

# REFERENCES

1. <https://www.geeksforgeeks.org/how-does-the-blockchain-work/>
2. Rahayu, Syarifah Bahiyah, et al. Military Blockchain for Supply Chain Management - JESOC.<https://www.jesoc.com/wp-content/uploads/2019/08/KC13_015.pdf>.
3. M. McAbee, Ashley S., et al. Military Intelligence Applications for Blockchain Technology. <https://pdfs.semanticscholar.org/4db1/edd97c5867ced07692e4c1e277c0fa3205ae.pdf>.
4. <https://www.bbc.com/news/business-44341490>
5. Ali Dorri, Salil S. Kanhere, and Raja Jurdak, “Blockchain in Internet of Things: Challenges and Solutions”
6. Volkan Dedeoglu, Raja Jurdak, Guntur D. Putra, “A Trust Architecture for Blockchain in IoT”
7. Salil S. Kanhere, Raja Jurdaky and Praveen Gauravaram, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home”
8. Raja Jurdak, Ali Dorri, Salil S. Kanhere “Towards an Optimized BlockChain for IoT”.
9. K. Anderton, “The business of video games: Market share for gaming platforms in 2019 [infographic]”. Jun 2019. [Online].Available: [https://www.forbes.com/sites/kevinanderton/2019/06/26/the business-of-video-games-market-share-for-gaming-platforms-in-2019- infographic/6f39edfe7b25](https://www.forbes.com/sites/kevinanderton/2019/06/26/the%20business-of-video-games-market-share-for-gaming-platforms-in-2019-%20infographic/6f39edfe7b25)
10. C. Gough, “Number of gamers worldwide 2021 Aug 2019.[Online].Available: <https://www.statista.com/statistics/748044/number> video-gamers-world/
11. V. Buterin “Ethereum: A next-generation smart contract and decentralised application platform”, Dec 2014
12. W. Entriken and D. Shirley, “Eip 721: Erc-721 nonfungible token standard”,” Jan 2018.[Online].Available: <https://eips.ethereum.org/EIPS/eip-721>
13. V. Buterin and F. Vogelsteller Eip 20: Erc-20 token standard, Nov 2015. [Online]. Available: <https://eips.ethereum.org/EIPS/eip-20>
14. W. Radomski, A. Cooke, and P. Castongua Eip 1155: Erc 1155 multi token standard, ,” Jun 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1155 2020 Second International Conference on Blockchain Computing and Applications (BCCA)
15. <https://ethereum.org/en/nft/>
16. <https://www.toprankedlegal.com/nft-mechanism-and-legal-issues-of-nft-transactions/>
17. <https://www.analyticsinsight.net/nfts-basics-examples-uses-and-benefits/>
18. <https://aws.amazon.com/blockchain/nfts-explained/>
19. <https://news.bloomberglaw.com/ip-law/the-trendy-hot-nft-market-has-a-new-entrant-patents>
20. <https://thegivingblock.com/resources/what-is-nft-fundraising/>
21. Omar Ali, Mujtaba Momin, Anup Shrestha, Ronnie Das, Fadia Alhajj, Yogesh K. Dwivedi, A review of the key challenges of non-fungible tokens, Technological Forecasting and Social Change, Volume 187, 2023, 122248, ISSN 0040-1625, <https://doi.org/10.1016/j.techfore.2022.122248>.
22. <https://www.sciencedirect.com/science/article/pii/S0167811622000544>
23. <https://support.opensea.io/hc/en-us/articles/4408474998419>
24. <https://101blockchains.com/smart-contract-security-guide/>
25. Kathleen Bridget Wilson, Adam Karg, Hadi Ghaderi, Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity,Business Horizons,Volume 65, Issue 5,2022,Pages 657-670,ISSN 0007-6813, <https://doi.org/10.1016/j.bushor.2021.10.007>.
26. Guo Y, Liang C. Blockchain application and outlook in the banking industry. Financ Innov 2: 24.
27. Hassani H, Huang X, Silva E. Banking with blockchain-ed big data. Journal of Management Analytics. 2018 Oct 2;5(4):256-75.
28. Isaak J, Hanna MJ. User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer. 2018 Aug 14;51(8):56-9.
29. Su H, Jung C. Perceptual enhancement of low light images based on two-step noise suppression. IEEE Access. 2018 Jan 8;6:7005-18.
30. https://en.wikipedia.org/wiki/History\_of\_banking/