

## MODULE VI

### CHAPTER 6

# Blockchain Applications & Case Studies

**University Prescribed Syllabus w.e.f Academic Year 2022-2023**

Blockchain in IoT, AI, Cyber Security

**Self-learning Topics :** Applications of Blockchain in various domains Education, Energy, Healthcare, real-estate, logistics, supply chain

6.1	Blockchain in Internet of Things .....	6-2
6.2	Blockchain in Artificial Intelligence .....	6-5
6.3	Blockchain in Cyber Security.....	6-9
•	<b>Chapter Ends .....</b>	<b>6-13</b>

## ► 6.1 BLOCKCHAIN IN INTERNET OF THINGS

### Challenge of using Blockchain in IoT

- The sheer size of the blockchain is one of the potential challenges of using blockchain in IoT. IoT devices are frequently connected to the internet and can generate a large number of transactions that the blockchain must process.
- Another issue is that blockchain may not be able to handle the high volume of transactions generated by IoT devices. Integrating blockchain technology with IoT devices may also be difficult. Similarly, blockchain may be incapable of providing the security and trust required for IoT devices.
- However, as blockchain technology advances, these obstacles may be overcome.

### Benefits of Blockchain in IoT

- Data decentralization. The information collected by IoT is oftentimes stored and managed by centralized servers, which is a possibility for hacking the confidential data by third-party people. Moreover, the network might fall immediately.
- Enhanced privacy. The blockchain can even hide the connection between the devices, offering transaction validation without third-party implementation. Moreover, the blockchain can optimize the IoT protocols, and supply the encryption. This lowers the risks of data leaking and IoT network hacking.
- Enhanced data management. IoT networks should transfer huge amounts of data in real-time through devices, systems and platforms, which raises new challenges for data management. The blockchain allows the devices to transfer data directly, without server's, cloud's, or local database's help., This shortens the number of transactions at least for one third (device - other device - server / cloud / local network - device). Moreover, smart contracts can make most of the processes between IoT devices automatic.
- Better Automation Process: Blockchain coupled with IoT can oversee the automation process that includes data automation process that includes data analysis and prompt actions.
- Encryption for Multi-Factor Authorization: With the help of blockchain IoT, organizations can offer biometric-based multi-factor passwords or authorization methods.
- Collaborative Environment for Shared Economy: Blockchain can offer a secured hub for all the shared economy industries and use IoT devices to oversee the business processes.

Enhanced scaling. Decentralized blockchain networks share the workload, which provides an improved transaction processing and increases the coordination between billions of IoT devices that are connected to it. The ability to share the data also helps to scale.

Automatic connection. Blockchain technology helps to make the commands and messages in IoT automatic by the means of smart contracts. These computer algorithms are used within IoT devices for data analysis, IoT devices temperature measuring, and daily temperatures measuring. The other example is an automatic filling of custom documents or automatic duty checkout after passing the border.

### Use Cases

#### Supply Chain Management

- A supply chain network involves numerous stakeholders, and this is primarily the reason why delivery delay becomes one of the biggest challenges in the supply chain and logistics industry. This is where Blockchain and IoT enter.
- While IoT-enabled devices will allow companies to track shipment movement at every stage, Blockchain will provide transparency to the entire transaction. IoT sensors (for example, motion sensors, GPS, temperature sensors, etc.) can offer details about the shipment status.
- This information is then stored in the Blockchain network for transparency – once the data is recorded on the Blockchain network, all the supply chain stakeholders listed in the Smart Contracts can access to the information in real-time. Together, Blockchain and IoT can help improve the reliability and traceability of the supply chain network.

#### Pharmacy

- In the traditional centralized approach, exchanging information generated by IoT devices lacks the security standards and ownership of data. However, thanks to Blockchain IoT allows homeowners to manage the home security system remotely from the smartphone. Blockchain could elevate Smart Homes security by eliminating the limitations of centralized infrastructure.
- For instance, Telstra, an Australian telecommunication and media company, provides smart home solutions. The company has implemented Blockchain and biometric security to ensure no one can manipulate the data captured from smart devices. Naturally, when the data is saved on the Blockchain, only the authorized person/persons can access it.
- The transparent nature of Blockchain will further allow all the stakeholders to access and monitor all the stages of drug manufacturing and supply from their connected devices.

Enhanced scaling. Decentralized blockchain networks share the workload, which provides an improved transaction processing and increases the coordination between billions of IoT devices that are connected to it. The ability to share the data also helps to scale.

Automatic connection. Blockchain technology helps to make the commands and messages in IoT automatic by the means of smart contracts. These computer algorithms are used within IoT devices for data analysis, IoT devices temperature measuring, and daily temperatures measuring. The other example is an automatic filling of custom documents or automatic duty checkout after passing the border.

### Use Cases

#### Supply Chain Management

- A supply chain network involves numerous stakeholders, and this is primarily the reason why delivery delay becomes one of the biggest challenges in the supply chain and logistics industry. This is where Blockchain and IoT enter.
- While IoT-enabled devices will allow companies to track shipment movement at every stage, Blockchain will provide transparency to the entire transaction. IoT sensors (for example, motion sensors, GPS, temperature sensors, etc.) can offer details about the shipment status.
- This information is then stored in the Blockchain network for transparency – once the data is recorded on the Blockchain network, all the supply chain stakeholders listed in the Smart Contracts can access to the information in real-time. Together, Blockchain and IoT can help improve the reliability and traceability of the supply chain network.

#### Pharmacy

- In the traditional centralized approach, exchanging information generated by IoT devices lacks the security standards and ownership of data. However, thanks to Blockchain IoT allows homeowners to manage the home security system remotely from the smartphone. Blockchain could elevate Smart Homes security by eliminating the limitations of centralized infrastructure.
- For instance, Telstra, an Australian telecommunication and media company, provides smart home solutions. The company has implemented Blockchain and biometric security to ensure no one can manipulate the data captured from smart devices. Naturally, when the data is saved on the Blockchain, only the authorized person/persons can access it.
- The transparent nature of Blockchain will further allow all the stakeholders to access and monitor all the stages of drug manufacturing and supply from their connected devices.

## Smart Homes

- In the traditional centralized approach, exchanging information generated by IoT devices lacks the security standards and ownership of data. However, thanks to Blockchain IoT allows homeowners to manage the home security system remotely from the smartphone. Blockchain could elevate Smart Homes security by eliminating the limitations of centralized infrastructure.
- For instance, Telstra, an Australian telecommunication and media company, provides smart home solutions. The company has implemented Blockchain and biometric security to ensure no one can manipulate the data captured from smart devices. Naturally, when the data is saved on the Blockchain, only the authorized person/persons can access it.

## Automotive Sector

- Digitization has swept across all sectors of the industry, and the automotive industry is no exception. Today, automotive companies are leveraging IoT-enabled sensors to develop fully automated vehicles. The automotive industry is further inclined to connecting IoT enabled vehicles with Blockchain tech to allow multiple users to exchange crucial information easily and quickly.
- Also, the industry is readily exploiting Blockchain IoT use cases that can transform autonomous cars, smart parking, and automated traffic control for the better.
- NetObjex presents a compelling case in point by creating a smart parking solution by combining Blockchain and IoT. It has collaborated with PNI, a parking sensor company for real-time vehicle detection and finding possible parking spots in the parking area. The integration also automates payments using crypto-wallets.

## Difficulties faced while using blockchain in IoT

### Difficult choice of a consensus protocol

- To choose the best blockchain option for the IoT you will need to take into account that many mechanisms cannot be used in the modern IoT environment due to high requirements to the computing power, scaling difficulties, high fees etc.
- For instance, if you choose the Bitcoin or Ethereum Blockchain, then each transaction between the devices will cost 2-20 dollars. Since the IoT deals with thousands or even millions of transactions every day, a vast amount of money is necessary, which is a huge drawback. Furthermore, the blockchains are very picky in terms of validators, which is not appropriate for IoT, since IoT devices are tiny sensors with little computing power and limited functionality.

### **Weak data encryption**

- Encryption - is a crucial part of many modern applications, programs, and systems. Unfortunately, IoT devices cannot interact with systems and users and encrypt the data as blockchain does.
- One of the possible solutions to increase the encrypting security in IoT is providing the entropy encryption, based on quantum random number generation.

### **Scaling difficulties**

- The problem is that IoT networks continue their rapid growth, which means that more smart devices, more transactions, and more data should be processed. The connection between the IoT elements normally requires immediate data transferring. All this causes difficulties with scaling, especially for blockchains with poor working speed.
- The perfect architecture of a blockchain for the Internet of Things should process thousands of transactions per second and provide security for simple network nodes. This can be achieved in a few ways.
- Parallel computing. This processes a few transactions at a time and increases the transaction effectiveness. Moreover, when one chain gets too complicated, it can be divided on parallel chains to help the traffic. This computing method can be used for data collecting and analysis in the IoT, for vast amounts of data analysis, and side projects processing that require a lot of computing.
- Other solutions that increase the work speed of a blockchain. Protocols like Plasma and Plasma Cash, have the potential of increasing the work speed by using affiliate chains, parental chains, and root chains by also adding smart contracts that can interact with the main blockchain.
- No standard communication protocols. The traditional IoT network devices usually connect to the internet via secure and fast connection methods (wireless or wired), like DSL/ADSL, Wi-Fi, 4G and LTE. Smart devices for blockchain and IoT integration are usually connected to the internet via protocols with low bandwidth and energy consumption: 802.15.4, 802.11a/b/g/n/p, LoRa, Zigbee, NB-IoT, and Sigfox. However, these protocols are not designed to work with blockchains.

## **6.2 BLOCKCHAIN IN ARTIFICIAL INTELLIGENCE**

- AI and blockchain are proving to be quite a powerful combination, improving virtually every industry in which they're implemented.

- Blockchain and artificial intelligence are combining to upgrade everything from food supply chain logistics and healthcare record sharing to media royalties and financial security. The integration of AI and Blockchain affects many aspects, including Security – AI and blockchain will offer a double shield against cyber-attacks.
- AI can effectively mine through a huge dataset and create newer scenarios and discover patterns based on data behavior. Blockchain helps to effectively remove bugs and fraudulent data sets.
- New classifiers and patterns created by AI can be verified on a decentralized blockchain infrastructure and verify their authenticity. This can be used in any consumer-facing business, such as retail transactions. Data acquired from the customers through blockchain infrastructure can be used to create marketing automation through AI.

### **Benefits**

- Improved business data models
- Globalized verification systems
- Innovative audits and compliance systems
- Smarter finance
- Transparent governance
- Intelligent retail
- Intelligent predictive analysis
- Digital Intellectual Property Rights

### **Use Cases**

### **Smart Computing Power**

- If you were to work a blockchain, with all its encrypted knowledge, on a laptop you'd like massive amounts of process power. The hashing algorithms used to mine Bitcoin blocks, for example, take a "brute force" approach – which consists of systematically enumerating all possible candidates for the solution and checking whether every candidate satisfies the problem's statement before confirmatory a dealing.
- AI affords U.S.A. the chance to maneuver faraway from this and tackle tasks in a very a lot of intelligent and economical approach. Imagine a machine learning-based algorithm, which could practically polish its skills in 'real-time' if it were fed the appropriate training data.

### Creating Diverse Data Sets

Unlike computing based-projects, blockchain technology creates suburbanized, transparent networks that can be accessed by anyone, around the world in a public blockchain network situation.

By making Associate in Nursing API of APIs on the blockchain, it'd allow the communicating of A.I. agents. As a result, various algorithms may be designed on various knowledge sets.

### Data Protection

- Through knowledge, AI receives data regarding the globe and things happening thereon. Knowledge feeds AI, and through it, AI will be able to continuously improve itself. On the opposite aspect, blockchain is essentially a technology that allows for the encrypted storage of data on a distributed ledger. It allows for the creation of fully secured databases that can be looked into by parties who have been approved to do so.
- Medical or financial data are too sensitive to hand over to a single company and its algorithms. Storing this data on a blockchain, which can be accessed by an AI, but only with permission and once it has gone through the proper procedures, could give us the enormous advantages of personalized recommendations while safely storing our sensitive data.

### Data Monetization

- Another turbulent innovation that might be doable by combining the 2 technologies is that the validation of information. Monetizing collected data is a huge revenue source for large companies, such as Facebook and Google. Having others decide how data is being sold to create profits for businesses demonstrates that data is being weaponized against us.
- Blockchain permits the U.S.A. to cryptographically defend our knowledge and have it utilized in how we tend to see work. This additionally lets the U.S.A. legitimize knowledge in person if we elect to, without having our personal information compromised. This is important to understand to combat biased algorithms and create diverse data sets in the future.
- The same goes for AI programs that require our knowledge. For AI algorithms to learn and develop, AI networks will be required to buy data directly from its creators, through data marketplaces. This will create the whole method a way more truthful method than it presently is, without tech giants exploiting its users. Such a knowledge marketplace also will open AI for smaller corporations. Developing and feeding AI is implausibly pricey for corporations that don't generate their knowledge

### Trusting AI Decision Making

- Using blockchain technology, there are immutable records of all the data, variables, and processes used by AIs for their decision-making processes. This makes it far easier to audit the entire process.
- With the appropriate blockchain programming, all steps from data entry to conclusions can be observed, and the observing party will be sure that this data has not been tampered with.
- It creates trust within the conclusions drawn by AI programs. This is a necessary step, as individuals and companies will not start using AI applications if they don't understand how they function, and on what information they base their decisions.

### Financial services

- Blockchain and AI are transforming the financial services industry by enabling trust, removing friction from multiparty transactions, and accelerating the speed of transactions. Consider the loan process.
- Applicants grant consent for access to personal records stored on the blockchain. Trust in the data and automated processes for evaluating the application help drive faster closings and improve customer satisfaction.

### Supply chain

- By digitizing a largely paper-based process, making the data shareable and trustworthy, and adding intelligence and automation to execute transactions, AI and blockchain are transforming supply chains across industries and creating new opportunities.
- For example, a manufacturer can track carbon emissions data at the product or parts level, adding accuracy and intelligence to decarbonization efforts.

### Life sciences

- Blockchain and AI in the pharmaceutical industry can add visibility and traceability to the drug supply chain while dramatically increasing the success rate of clinical trials.
- Combining advanced data analysis with a decentralized framework for clinical trials enables data integrity, transparency, patient tracking, consent management and automation of trial participation and data collection.

Examples

**FINALIZE**

- Finalize is a software platform that uses blockchain and machine learning to build applications aimed at improving civil infrastructure. The company's tools automate and speed up construction industry workflow, management, and verification processes, and its technology also integrates with wearables to meet safety regulations.
- Finalize aims to make crucial processes more efficient while maximizing ROI in an industry whose revenues are projected to hit \$15.5 trillion by 2028.

**BLACKBOX AI**

- Blackbox AI develops artificial intelligence tools for emerging technologies. The company's engineers create a customized information architecture that powers everything from machine learning and natural language processing to blockchain tools.
- Besides developing infrastructure for blockchains, the company also offers consultation services that focus on how their products can maximize a blockchain's potential. Blackbox AI's engineers are from some of the largest tech organizations in the world (including Apple, Intel, NVIDIA and MIT), and they have devised AI-based tools for everything from virtual reality to natural language processing.

**6.3 BLOCKCHAIN IN CYBER SECURITY****Blockchain Cybersecurity Usage****1. Blockchain for threat intelligence**

Threat intelligence is an advanced process which involves gathering valuable insights including mechanisms, context, indicators, actionable advice and implications about an emerging or existing cyberthreat. Threat intelligence processes must be adapted to a company ecosystem to integrate it properly.

**2. Blockchain for backup and recovery**

One of the most innovative applications of blockchain technologies is to use it by secure storage and recovery systems.

### 3. Internet of things.

#### Use Cases

1. **IoT security :** With the increasing application of AI and IoT, the security of data and systems from hackers has always been a major concern. Usage of Blockchain for improved security by using device-to-device encryption to secure communication, key management techniques, and authentication is a potential use case to maintain cybersecurity in the IoT system.
2. **The integrity of software downloads :** Blockchain can be utilized to verify updates and installers to prevent malicious software from infecting the devices. Here, hashes are recorded in the blockchain and new software identities can be compared to the hashes to verify the integrity of the downloads.
3. **Data transmission protection :** By using encryption, the data in transit will be protected from unauthorized access.
4. **Decentralized storage of critical data :** With the exponentially increasing data generated every day, blockchain-based storage solutions help achieve decentralized storage thus protecting digital information.
5. **Mitigating DDoS Attacks :** One of the most popular cyberattacks today is DDoS attacks where hackers aim to generate a flood of Internet traffic and thus disrupt the flow of services. The properties of immutability and cryptography help Blockchain prove to be an effective solution for these attacks.
6. **DNS security :** The Domain Name System (DNS) is similar to a public directory that links domain names to their IP addresses. Over time, hackers have tried to access the DNS and exploit these links thus crashing sites. Due to Blockchain's properties of immutability and decentralized systems, the DNS can be stored with enhanced security.

#### Application of Blockchain in Cybersecurity

In cybersecurity, the CIA triad model acts as a reference to assess the security model of an organization. The triad consists of-

1. Confidentiality
2. Integrity
3. Availability

Blockchain helps us ensure all these policies are satisfied.

1. **Confidentiality :** It means to ensure that only interested and authorized parties access the appropriate data. Full encryption of blockchain data ensures that the data will not be accessible by unauthorized parties while flowing through untrusted networks. Security measures such as access controls should be implemented directly at the application level so as to prevent attacks from within the network. Blockchain can provide advanced security controls by using public key infrastructure to authenticate parties and encrypt their communication. However backup storage of private keys in secondary storage poses theft of private keys as a high risk. To prevent this, key management procedures such as IETF or RFC and cryptographic algorithms based on integer factorization problems should be implemented.
2. **Integrity :** Blockchains built-in characteristics of immutability and traceability help organizations ensure data integrity. Consensus model protocols can further help organizations to implement mechanisms to prevent and control ledger splitting in the event of a 51% cyber control attack. In Blockchain, with every new iteration, the previous state of the system is stored thus providing a fully traceable history log. Smart contracts can be used to verify and enforce rules between parties preventing miners from mining blocks of data.
3. **Availability :** In recent times, cyberattacks attempting to impact technology services availability are on the surge with DDoSs being the most common types of attacks. However, in blockchain-based systems, DDoS attacks are costly as the attacker attempts to overpower the network with a great number of small transactions. Blockchains have no single point of failure which decreases the chances of IP-based DDoS attacks disrupting the normal operation. Data remains available through various nodes and thus full copies of the ledger can be accessed at all times. The combination of multiple nodes and distributed operation makes the platforms and systems resilient.

### **Pros of using Blockchain in Cybersecurity**

1. **User confidentiality:** The public key cryptography in a Blockchain network helps maintain the confidentiality of the users.
2. **Data transparency and traceability:** A history of all these transactions is maintained and thus can be traced anytime. The transactions data is digitally signed by members of the Blockchain network thus maintaining transparency.
3. **Secure data storage and processing:** Blockchain's major feature of immutability and records of any changes to the data help store the data in a safe and secure manner.
4. **No single point failures:** Blockchain systems are decentralized and thus a single node failure doesn't affect the entire network. Thus even during DDoS attacks, the system is not compromised due to the maintenance of multiple copies of ledgers. This advantage is not possible for Private blockchains.

5. **Safe data transfers:** The Public Key Infrastructure (PKI) in Blockchain maintains authentication during data transfers. Smart contracts help with the automatic execution of agreements between two parties during a transfer.

#### **Cons of using Blockchain in Cybersecurity**

1. **Reliance on private keys :** Blockchains rely heavily on Private Keys for encryption of data but these private keys cannot be recovered once lost. This may lead to losing access to encrypted data forever.
2. **Adaptability and scalability challenges :** Blockchain networks have preset block volume and limits to transactions per second so it becomes very important to check the scalability of the network. Integrating Blockchain technology requires a complete replacement of the current systems and thus companies may face difficulties in doing so.
3. **High operating costs :** Blockchain requires high computing power and storage capabilities. This leads to higher costs as compared to non-Blockchain applications.
4. **Lack of governance :** Blockchain concepts aren't regulated globally yet. Regulations and frameworks need to be developed in order to maintain governance in Blockchain applications.
5. **Blockchain literacy :** Learning Blockchain technology requires a profound knowledge of various development, programming languages, and other tools. Thus in spite of numerous applications of Blockchain Technology, enough Blockchain developers are not available in the present scenario.

#### **Real-Life Application Examples**

Following are some prominent examples where Blockchain is used for Cybersecurity:

1. **Barclays (London, England), Traditional Banking:** Barclays have filed a patent to use blockchain to enhance security in fund transfers. It aims to stabilize cryptocurrency transfers by using Distributed Ledger Technology (DLT). Thus, blockchain helps the bank store customer information on a secure blockchain.
2. **CISCO (San Jose, California), IoT:** Cisco plans to use blockchain to secure IoT devices as ledger technology eliminates single point of failure and encryption helps secure data.
3. **Coinbase (San Francisco, California), Cryptocurrencies:** Coinbase uses encryption to store wallets and passwords in a secure database. It also undergoes background checks on employees to ensure that their crypto is secured.

- 4. **Australian Government (Canberra, Australia):** The Australian government has plans to develop a cybersecurity network based on DLT. The government has also partnered with IBM to secure the storage of government documents with the creation of a blockchain ecosystem.
- 5. **Philips Healthcare (Andover, Massachusetts), Healthcare:** Philips Healthcare has partnered with hospitals all over the world to create a healthcare ecosystem using blockchain and AI. This ecosystem will help discover and analyze various operational, administrative, and medical data.
- 6. **Chinese Military (Beijing, China), Defense and Military:** China's government and the military are attempting to secure vital government and military information, intelligence information using blockchain cybersecurity.
- 7. **Founders Bank (Valletta, Malta), Cryptocurrencies:** They aim to be the world's first decentralized bank thus being owned by the buyers and not any central authority. Concepts such as encryption and distributed ledgers will be used to store and secure users' cryptocurrencies.
- 8. **The State of Colorado (Denver, Colorado), Government:** According to a bill passed by the Senate, the government will consider using Blockchain to secure the storage of records thus trying to curb the increase in attempted attacks.
- 9. **J. P. Morgan (New York, NY), Traditional Banking:** They have developed a platform called Quorum which uses Blockchain to process private transactions. It uses the concepts of Smart contracts and cryptography to maintain the security of the transactions.
- 10. **Health Linkages (Mountain View, California):** They aim to use Blockchain to keep patient records secure allowing only certain personnel to access the records. It will also be used to maintain a chronological record of major healthcare events which will help doctors make better decisions.

---

Chapter Ends...

