

Fundamentals of Blockchain

Prepared by Dr. Omar Al-kasasbeh

FNT628

Blockchain and Cryptocurrencies

Lecture 1



Blockchain and Cryptocurrencies

FNT 628

Blockchain and Cryptocurrencies

Prepared by
Dr. Omar Al-kasasbeh

Fundamentals of Blockchain

The need for humankind to perform a process with perfection and accuracy commenced with the origin of computers. The digitalized computing machines, initialized in the 1940s, merely carried out arithmetic operations marking the first step towards the innovative computers of today. Computers are part of our day-to-day life now. Computer networks connect not only computers around the globe but also, human beings across the world. Today we are at the Fifth Industrial Revolution with over 50% of the world connected via the internet and technology progressing at its most sophisticated phase with Artificial Intelligence, Big Data, virtual reality, and one of the most disruptive technologies the Blockchain, forming the bedrock of such development.

What is Blockchain

Technically, Blockchain is defined as a distributed, replicated peer-to-peer network of databases that allows multiple non-trusting parties to transact without a trusted intermediary and maintains an ever growing, append-only, tamper-resistant list of time-sequenced records. In short, Blockchain is a type of distributed ledger that sits on the internet for recording transactions and maintaining a permanent and verifiable record-set of information. This innovative technology was first published in 2008 by Satoshi Nakamoto in a white paper titled “A Peer-to-Peer Electronic Cash System.” The thought behind the design was to create a decentralized digital currency that is free from government regulation whereby two people can confidently trade directly with one another without the need for mediators or intermediaries. In 2009, the concept became a reality when Satoshi Nakamoto implemented the first application of the Blockchain we all know as Bitcoin.

Lecture

1

The Bitcoin and the Blockchain

To better understand the difference between Bitcoin and Blockchain, let us delve a little bit into what they are and what they are not.

1) Meaning

Bitcoin is a cryptocurrency, while Blockchain is a ledger or database of information. Bitcoin was created to reduce the government's control over cross-border transactions and to speed up the transaction process by removing the need for third-party intermediaries.

2) Scope of Usage

Bitcoin is limited to currency transactions, while the blockchain has numerous applications.

The Bitcoin and the Blockchain

3) Transparency

Bitcoin has a high degree of anonymity. Though the transactions are visible, it is close to impossible to identify the user. Until today, the identity of Satoshi Nakamoto is a mystery even though Satoshi has roughly million bitcoins (BTC) worth around 8 billion dollars as of 2019. On the other hand, Blockchain is quite transparent as it is expected to work across multiple industry applications. However, Smart contracts and various consensus mechanisms, Blockchain can assure compliance to KYC and other industry standards.

The Evolution of Blockchain

Understanding the evolution of blockchain helps us comprehend how this technology has reached its current state and the problems that each generation has attempted to address.

a) First Generation Blockchain (2008-2013): The Origin of Bitcoin In 2009, Bitcoin became the first application of Blockchain technology. Satoshi Nakamoto formed the Genesis block. On 12 Jan 2009, the first successful bitcoin transaction on the blockchain takes place between Nakamoto and Hal Finney. The first generation of blockchain promised transparency, immutability, accountability, and security in transactions. However, the protocols used necessitated the use of heavy mining hardware and significant resources leading to problems in scalability, interoperability, and speed. To date, Bitcoin is one of the slowest cryptocurrency, taking about 10 minutes to confirm a transaction.

The Evolution of Blockchain

b) Second Generation Blockchain (2013-2015): Transactions with Smart Contracts

The second-generation sought to overcome the limitations of the Bitcoin. Thus emerged Ethereum in 2013, when it was realized that the underlying technology of Bitcoin could be used for all kinds of B2C and other general applications. It still used the Proof-of-work algorithm and had less-than-optimal speed. Though Ethereum required lesser energy to maintain, there were still concerns about future scalability. However, with the hosting of Smart Contracts that made available new functionalities, Ethereum was the go-to blockchain for Enterprise use.

The Evolution of Blockchain

c) Third Generation Blockchain (2015-2018): Distributed Applications

This generation saw the arrival of Hyperledger from the Linux Foundation and Decentralized Applications (DApps) of Ethereum. Though the Hyperledger is a platform that can plug in any consensus mechanism, Smart Contracts of Ethereum opened up the possibility of a Proof-of-Stake consensus mechanism. The focus of the generation was consensus mechanisms that can bring greater interoperability and boost network speeds. Promoting cross-chain transactions, using sharding (a type of database partitioning that separates vast databases into smaller, faster, and more easily managed parts) and establishment of parallel chains are only some of the approaches being taken by the third generation blockchain solutions.

The Evolution of Blockchain

d) Fourth Generation Blockchain (2018–Future)

Blockchain technology's future appears optimistic as many governments and organizations are investing heavily in innovations and applications. A significant innovation on the horizon is called blockchain scaling. A scaled blockchain is expected to accelerate the processing speeds, without sacrificing security significantly. This is done by assessing the computing power required to validate each transaction and then dividing the work efficiently. Progress in this front is yet to be seen, but the outlook has been positive and more is expected on this front.

Lecture

1

How Blockchain Technology Works

One of the features in the blockchain is digital trust. In the digital world, trust relates to two questions: “Are you whom you say you are?” and “Do you have the right to do what you want to do?” This boils down to proving identity (authentication) and proving permissions (authorization). Authentication is addressed with cryptography. Blockchain utilizes public-key or asymmetric cryptography that involves a public key and a private key. When a private key is created, its public key pair is also created using a complex algorithmic process. Both the public key and private keys are generated and stored in a place referred to in the Blockchain world as “wallet.” The Wallet is a software program that not only stores your private and public keys but also facilitates the sending and receiving of cryptocurrency through the blockchain, while also monitoring your balance.

Lecture

1

While the private key must be maintained confidential, the public key may be distributed to anyone. You can relate the public key to your bank account number that you would need to share to receive money while your private key is similar to your bank account password or PIN that only you can access. So, if anyone sends you a message with your public key, only you can open it with your private key provided no one else has access to your private key. Thus, it goes without saying that the private key should not be shared with anyone.

Lecture

1

components of Blockchain

So far, we learned about the origin of Blockchain, its inherent concepts and the technologies that make blockchain transaction secure, immutable, and indisputable. But from where does blockchain get its name, and what makes it unique? To understand the block in Blockchain, we need first to understand some of the concepts, terms, and components used in Blockchain technology.

Lecture

1

1. Node

A node is an electronic device (computers, mobile devices, servers, etc.) that is connected to the internet. In blockchain parlance, any computer or hardware device that is connected to the blockchain network is a node. All the nodes in the network have a copy of the blockchain ledger and are interconnected. So theoretically, we can say that the Blockchain exists on nodes whose primary purpose is to preserve the integrity of the blockchain. The node supports the network by maintaining a copy of the blockchain. A node can be:

A- A Full Node

The node maintains a full copy of the transaction history of the blockchain. Computers run full nodes to help synch the blockchain. They also help the network by processing and accepting transactions/blocks, validating those transactions/blocks, and then broadcasting them to the network.

b) Light Node

Nodes maintain only a partial copy of the ledger as they could be early users or those who do not have sufficient disk space for the full blockchain. Light nodes download only the block headers to validate the authenticity of transactions using a method called SPV or Simplified Payment Verification. They rely on the full nodes for the latest headers, account balance, and any transaction that affects their wallet.

2. Ledger

A ledger, in blockchain technology, refers to a digital database of information that is immutable. Blockchain is commonly referred to as a public distributed decentralized ledger. Let us see why.

a) Ledger Is Public

Anyone in the blockchain has access to the ledger and can read or verify the transactions therein.

b) Ledger Is Distributed

All the nodes in the blockchain network have a copy of the blockchain ledger. The traditional database works in a client–server environment, while the blockchain works on the principle of replication in every node.

c) Ledger Is Decentralized

Blockchain protocols are built such that no one node or group of nodes has excessive control over the ledger. There is no central control; hence it is decentralized with no single point of failure. So, while the traditional database works on central principle integrity (only the central body can validate the record), the blockchain works on the principle that anybody can validate the records. Also, the traditional database works on the CRUD (Create, Read, Update, Delete) principle

3- Wallet

A Wallet in the blockchain world is a digital wallet that allows users to manage cryptocurrency like bitcoin, Litecoin, ether, etc. With a blockchain wallet, one can receive and send cryptocurrency. The term “wallet” is a misnomer, as real money is not stored. When Person A sends cryptocurrency coins to Person B’s wallet, Person A is, in effect, signing off ownership of the coins to Person B. However, Person B can spend the coins only if the private key stored in Person B’s wallet matches the public address the cryptocurrency is assigned to. If the keys match, the balance in Person B’s wallet increases while that in Person A’s wallet decreases accordingly. It should be noted that there are no real coins at play here. The said transaction is a new record added on the blockchain along with a change in the balance in the cryptocurrency wallet

Lecture

1

a) Privacy is Maintained

Whenever a user creates a wallet, the public and private key associated with the wallet is also generated. It can be compared to how your email account works. The public key is like email id, and the private key is your email id password. Just like you share your email id to receive an email, you share your public key to receive funds. However, your identity and personal details are kept private

b) Transactions are Secure

The private key is used to send funds as well as to open encrypted messages. This keeps the transactions secure.

c) Ease of Usage

Wallets can be installed and accessed from the web, desktop, or any mobile device. Transfer of funds is relatively instantaneous, without any geographical constraints or intermediaries like banks.

d) Currency Conversion

Wallets help you to transact across various types of cryptocurrencies like BTC, ETH, XMR, LTC, and others, without worrying about the currency conversion.

Lecture

1

4 Nonce

A nonce is a number generated randomly that can be used just once in the cryptographic communication. Adding a nonce to a transaction's identifier makes it additionally unique, thus reducing the chance of duplicate transactions. Nonce is the key to creating a block in a blockchain database.

5 Hash

A hash function can take data of any size, perform an operation on it, and return a “hash” that is a data of a fixed size. Whether it is a single sentence or the Oxford Dictionary, the resulting hash will always be of the same size. Critical characteristics of hashing are:

6 Mining

Mining is the mechanism whereby nodes called “miners” in the Bitcoin world or “forgers” in the Ethereum world validate new transactions and add them to the blockchain ledger. Miners/forgers compete to solve a complex mathematical problem based on a cryptographic hash algorithm referred to earlier, basically the nonce and hashing. Mining comprises hashing a block and then introducing a nonce to the hashing function and running the hash all over again. However, this is where the complexity occurs: The resulting hash value should be less than the target value.

Lecture

1

This process is run multiple times until the required hash is reached. Once the solution is found, the new block is added to the network and propagated.

Miner nodes compete to solve a complex mathematical problem using massive computing power, energy, and time.

The first miner to create the winning hash will receive rewards in the form of transaction fees or new bitcoins. This process of computing the hash is called proof-of-work or consensus mechanism and provides integrity to the blockchain.

Lecture

1

Consensus Protocol

Consensus protocols are a set of rules whereby nodes in a network can achieve agreement on the data value or state of the network such that it benefits the network as a whole and does not focus on individual interests. In the decentralized world of Blockchain technology, all the participating nodes must agree on a single source of truth, for example, whether Joe has enough money in his wallet or he is double-spending. Consensus protocols are used in blockchain to ensure that all transactions are validated before being added to the blockchain, i.e., there should be a 'consensus' or agreement between the nodes on the network on the state of a blockchain. This allows for three critical functions of the blockchain:

Lecture

1

Consensus Protocol

- a) To make sure all nodes agree on the correctness of the data and the state of the blockchain.
- b) Spread control between nodes, thus preventing any single entity from taking control or disrupting the blockchain system. Consensus rules aim to guarantee that a single chain is used and followed.
- c) They are designed to be costly and resource-heavy in terms of computing power, energy, and time, in an effort to keep the network honest. Proof-of-Work (PoW) algorithm is used in Bitcoin protocol, while Proof-of-Stake (PoS) algorithm is in the Ethereum Casper Protocol.

Lecture

1

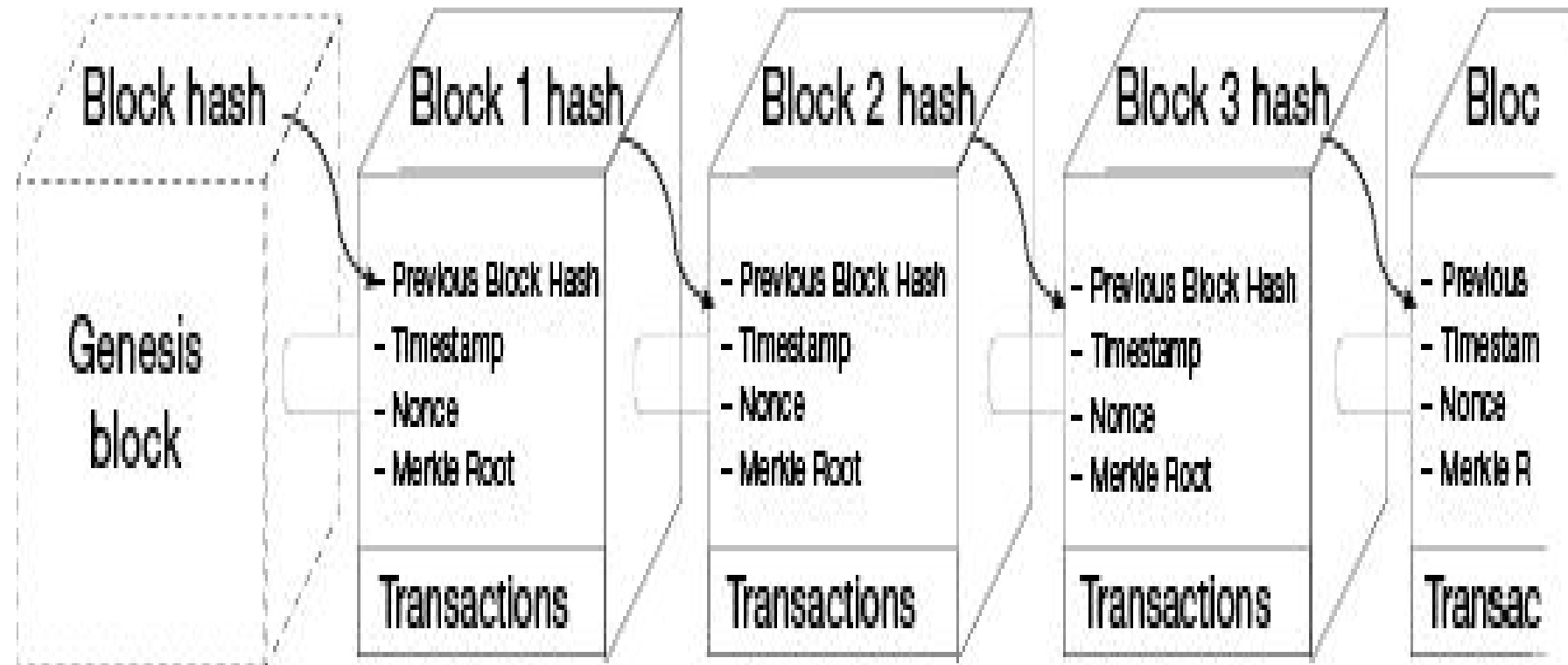
Meaning of the Block

The block is a record that contains the transaction data details. It comprises of the following details:

- 1) Hash of the block Alphanumeric number to identify the block
- 2) Hash of the previous block
- 3) Timestamp
- 4) Nonce the random number used to vary the value of the hash
- 5) Merkle root hash of all the hashes of all the transactions in the block
- 6) Transaction data. This contains details of several transactions

Lecture

1



Lecture

1

The genesis block is the first block. It is the only block with no data hash of the previous block because no block precedes it. The genesis block contains transactions that are combined and validated to produce a unique hash. The genesis block hash, along with all the new transactions, are processed and used as input to create a new hash that is used in the next block, i.e., say Block 1. Block 2 hash is created with a hash of Block 1 and another set of new transactions.

Lecture

1

This goes on with each block linking back to its previous block via its hash, thus forming a chain leading back to the genesis block. Hence the name, blockchain. This continuous linkage makes it impossible for any malicious actor to alter the information or to insert a block between two existing blocks. To do so, all connected blocks would need to be altered as well. As a result, each block strengthens the previous block, including the security of the entire blockchain, because a bigger chain means more blocks would need to be changed if one wants to tamper with any information.

Lecture

1

With the ever-growing popularity of blockchain, more and more people are moving towards transacting in digital currency. This brings about the double-spend problem, a flaw that is unique to digital currencies. Double-spending, as the name suggests, is spending the money more than once. Just as one can copy a digital file and send it to several people, it is possible to duplicate crypto coin or token and reuse it. If this occurs in the blockchain network, it could not only breakdown the concept of trusted distributed ledger but also lead to inflation with fraudulent, duplicate currencies in the network.

Lecture

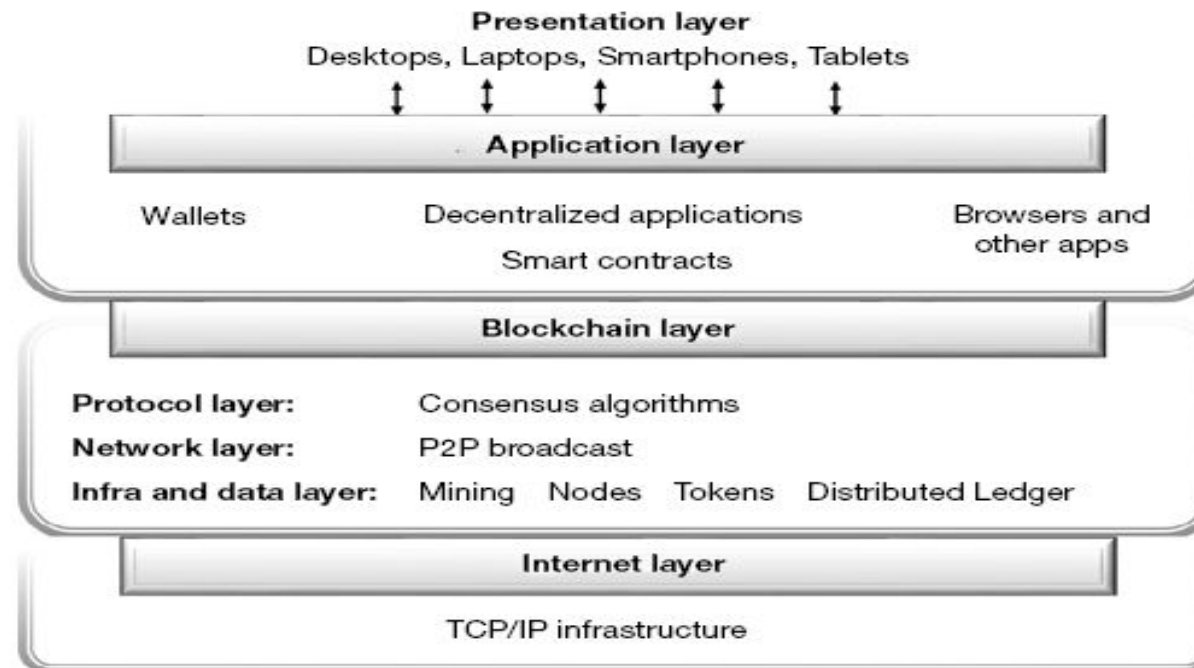
1

Going back and attempting to double-spend that transaction would require the same if not more computational power, especially with more blocks added to the chain in the interim; it is practically impossible to modify all the blocks. No one will expend enormous amount of resources if the payback is not worth the effort. Also, the first transaction would be time-stamped and cryptographically linked to previous blocks and broadcasted to all nodes in the network. When the second (fraudulent) transaction is proposed, it will fail at the verification process and be rejected. Once a transaction is confirmed, it is nearly impossible to double spend it. The more confirmed blocks in the chain, the harder it is to double-spend the crypto.

Lecture

1

A simple structure of the blockchain ecosystem is represented in Fig.2 It typically consists of:



Lecture

1

a) The Presentation Layer

This layer is a door to users that gives access to the whole network and blockchain applications. The UI (User Interface) and UX (User Experience) of the blockchain app come into play here. In today's competitive market, mobility and ease of usage are paramount to customer satisfaction. It is no different for blockchain where UI and UX design could make or break a blockchain adoption. A good UX design will enhance customer satisfaction and loyalty by improving the product usability and interaction between the user and the rest of the blockchain ecosystem or company. This could relate to faster speeds, relevant information, etc. UI design produces blockchain visuals or graphical presentations.

b) The Application Layer

This is the layer that combines the business logic with user interactions. It consists of the Decentralized Application, better known as DApps running on a P2P network. It is the DApps that sets the communication between the Presentation and Blockchain layers. DApps is similar to a web application except that while APIs are used to connect a website to a database, DApps connects to the Blockchain via Smart Contracts. The Smart Contract is a program containing a set of rules and criteria that automatically execute if/when the pre-defined conditions are met. More on Smart Contracts and DApps are explained in other chapters within this book.

Lecture

1

c) The Blockchain Layer

This is where the core of the blockchain subsists. It consists of the consensus algorithms (PoW, PoS, pBFT, etc.), the medium, and interface for the P2P network that decide how data is packetized and transmitted between peers. It controls the mining layer, protocols that decide the consensus methods and participation, nodes that execute protocols, and the distributed ledger.

d) The Internet Layer

Blockchain works over the internet. This layer ties all the networks together, i.e., the computers, IoT devices, smartphones, etc.

Lecture

1

Potential Applications in the Industry

The issues relating to blockchain technology may be significant, but its inherent benefits of immutability, openly shared ledger, security and non-dependence of intermediaries means that blockchain cannot be ignored. All agree that blockchain is way faster than the manual validation and audit process. Following are some of the potential applications that could cut across any industry and revolutionize the way we do business:

Lecture

1

a) Digital Identity

In today's world, proof of identity is a must for verification; be it your security number, passport, birth certificate, driver's license, etc. Without a valid form of id, one cannot open a bank account, own property, get government services, or employment. Digital identities on the blockchain can reduce the burden of maintaining physical copies or ID cards and protect from identity theft, providing control over your own identity (to share only specific information that is relevant for the purpose). Blockchain technology can provide a breakthrough for helping people who do not have legal identities such as refugees and people who live way below the poverty line and do not have ids. Elections are another area that could benefit from digital identity.

b) Payments and Settlement

Swiss bank UBS and UK-based Barclays are exploring blockchain solutions as a means to expedite back-office functions and settlement. Some in the banking industry say this could cut up to \$20B in middleman costs. Banks and other financial sectors are exploring various cases of possible blockchain use in areas such as payments and settlement of currencies, asset registries, enforcement and clearing derivative contracts, regulatory reporting, KYC, AML registries, improving post-trade processing services, etc.

Lecture

1

c) Proof of Ownership

Blockchain can be used to track any asset, be it jewelry, property deeds, vehicle, paintings, or any artefact, for proof of ownership. Fake and stolen goods are a significant issue impacting global commerce. Currently, proof of ownership is mostly paper-based that can be stolen or faked. With blockchain, all the properties of the asset can be digitized and stored in the blockchain. As the blockchain ledger is public and immutable, the ownership of the asset can be tracked to ensure its authenticity. This aids consumers and insurance companies in terms of time and money for evaluations, legal purchases, and arbitration.

d) Records Management

Industries that rely on the manual process of verification that is heavy on paper documentation and case-by-case checking can leverage blockchain technology. The education industry can benefit from blockchain solutions for verifying academic credentials, thereby reducing fraudulent claims of unearned educational qualifications. In healthcare, vast volumes of patient data can be stored securely and made accessible only to verified authorities, thus ensuring the privacy of patient data. The blockchain can securely store intellectual property and creative digital products like music, photos, software apps, etc.

e) Supply Chain Management

The undisputable nature of blockchain data makes it possible to track the journey of a product/product starting from its origin to its destination. There is hardly any industry without a supply chain, be it pharmaceuticals, food & beverages, automotive, construction, etc. When all parties see the same data and can verify shipment, receipt, and customs clearance, this cuts cost and streamlines the whole system. By using blockchain technology and removing paper-based trails and intermediaries, businesses can quickly pinpoint inefficiencies within their supply chains in nearly real-time. Contaminated products can be tracked and traced back to the source for containment and prevention.

Lecture

1

Summary



Thank You