**YOU DON’T KNOW BLOCKCHAIN**

**INTRODUCTION**

It is obvious you’ve heard the term Blockchain Technology or Blockchain for short but how do you really understand this concept? Most people also buy and sell or trade Bitcoin, Ethereum and other cryptocurrencies but don’t understand the behind the scenes of whatever that happens. Blockchain is a relatively new technology that is gaining popularity and change how businesses, finance, government, health, media and other industries operate.

Through out this course, we learn and understand the blockchain technology, Bitcoin, Ethereum, Smart Contracts, Mining, Decentralized Apps (DApps), Tokens etc.

We’ll start the course by understanding blockchain technology and other concepts will follow.

NB: This course is not to make you a blockchain master but to help you understand the blockchain technology, what it is and what it’s not.

I won’t discuss how to trade or buy and sell Bitcoin, Ethereum or any other cryptocurrency here.

This course is to make you a **BLOCKCHAIN LITERATE.**

THANK YOU FOR EMBARKING ON THIS JOURNEY WITH ME!!!

**PART 1: BLOCKCHAIN**

This chapter is an introduction to blockchain technology, the fundamentals and theories behind it, the various concepts that have been combined to build the **Blockchain.**

In the year 2008, when Bitcoin was invented the world was introduced to a new concept which revolutionized the whole society. It was something that aims to impact upon every industry. This new concept was **Blockchain**, the underlying technology that powers Bitcoin.

Bitcoin was the first technology that was successfully built on the blockchain.

In 2008, a paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System, was written by an unknown person or group called Satoshi Nakamoto.

This paper can be viewed on the bitcoin.org website via the link: <https://bitcoin.org/bitcoin.pdf>.

No one knows the actual identity of Satoshi Nakamoto.

Before I begin to explain to you what Blockchain is, first, I would like to touch on Bitcoin, as there is a myth going around that Bitcoin equals Blockchain. Well, that is incorrect. Though, it is often referred to as the same thing. Bitcoin is cryptocurrency, digitized money, that is allowed and kept alive due to the technology called Blockchain. When Blockchain technology began to exist, the first application that was tested on the platform was Bitcoin. Because Bitcoin was the first application on the Blockchain technology, one might say that Bitcoin is Blockchain, and that could make sense. However, Blockchain is not Bitcoin. I hope that makes sense. Blockchain is so complex that still there are very few human beings who understand each part of it. In fact, Blockchain is so complicated that we (as humans) keep on finding more and more ideas that this technology can solve every day. We could say that Blockchain is solving problems.

**WHAT IS DECENTRALIZTION?**

Decentralization in blockchain simply means that no single central authority is in control of the network.

WHAT IS A DISTRIBUTED SYSTEM?

Understanding distributed systems is essential to our understanding blockchain, as blockchain was a distributed system at its core. It is a distributed ledger that can be centralized or decentralized.

**Distributed systems** are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome. It is modeled in such a way that end users see it as a single logical platform. For example, Google's search engine is based on a large distributed system; however, to a user, it looks like a single, coherent platform.

**WHAT IS BLOCKCHAIN?**

BLOCKCHAIN is a peer-to-peer, decentralized, distributed ledger that is secure by cryptography, immutable and updated only via consensus among peers.

This means that the blockchain is just like a database that is held my individuals, which has no central controller and data can only be added to it if only there’s a total agreement between all individuals who are part of the blockchain network.

Create, Read, Update, Delete (CRUD) operations on traditional databases cannot be performed on the blockchain. That is, you cannot update or change any data on the blockchain after it has been appended.

To change something on the blockchain is very difficult and sometimes almost impossible to do.

NB: We will learn how data on the Bitcoin or Ethereum blockchain can be changed later through **soft and hard fork.**

**COMPONENTS OF A BLOCKCHAIN**

1. Address: Addresses are unique identifiers used in a blockchain transaction to denote sender and recipients.
2. Transaction: It is a fundamental unit of a blockchain. A transaction represents a transfer of value from one value (usually cryptocurrencies like Bitcoin or Ether) from one address to another.
3. Block: It contains multiple transactions and other elements such as previous block hash of a block header, timestamp and nonce (number once).

Other elements of a block include:

* 1. A reference to a previous block except the genesis block.

NB: Genesis Block is the first block in the blockchain that is hardcoded at the time the blockchain was first started or constructed.

* 1. Nonce is a number that is generated and used only once. It is value that is used to authenticate a block through Proof of Work (PoW) consensus algorithms.
  2. A timestamp is the creation time of the block.
  3. Merkle root is a hash of all the nodes of a merkle tree. Merkle trees are used to allow efficient verification of transactions.

1. Peer-to-Peer Network: This is a network where all nodes can communicate with each other and send and receive messages.
2. The Scripting or Programming language: Scripts perform various operations on a transaction in order to facilitate various functions. In Bitcoin, transactions are predefined in a language called Script, which consists of commands to allow nodes to transfer bitcoins from one address to another.

NB: Bitcoin’s Script language cannot be used in the development of other programs on the blockchain because it is not **Turing Complete.**

A Turing Complete Language means that it can perform any computation. It is named after Alan Turing, who developed the idea of a Turing machine that can run any algorithm however complex.

Ethereum’s Solidity Language is Turing Complex, that is it can be used to build other programs called **smart contracts** on the Ethereum blockchain.

1. Virtual Machine: It allows smart contracts to run on a blockchain such Ethereum Virtual Machine (EVM).
2. Smart Contracts: These are programs or code snippets that run on top of the blockchain and contains the business logic to be executed when certain conditions are met.
3. Node: A node has different functionalities on a blockchain.
   1. It can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain.
   2. Nodes can perform simple transaction verifications etc.
4. Transaction Fee: Validating nodes in a blockchain, also known as miners, need to perform some work in order to include the transactions in the blockchain. Thus, they need to have an incentive to do this work, and this incentive can be paid in the form of transaction fees.

The transaction fees don't depend on how big is the transaction in terms of amount.

**HOW BLOCKCHAIN WORKS**

Nodes are either miners who create new blocks and mint cryptocurrencies. They can also validate and digitally sign the transactions. A critical decision that every blockchain network has to make is to figure out which node will append or add the next block to the blockchain. This decision is made using a consensus mechanism. Consensus mechanism will be explained later.

Now how does a blockchain validate transactions and creates and adds blocks to grow the blockchain?

1. Transaction is initiated or started: First a node starts a transaction by creating it and digitally signing it with its private key. Usually, this is a transfer of value between users on the blockchain network. Maybe the transfer of Bitcoin from Person A to Person B.
2. Transaction is validated and broadcast: A transaction is disseminated through a protocol to other nodes or peers on the blockchain to validate it.
3. Find new block: When the transaction is validated by nodes or miners it is included in the block and the process of mining starts.
4. New block found: Once a miner solves a mathematical puzzle (implementation of consensus mechanism), the block is considered found or mined. Usually, miner who solves the mathematical puzzle is rewarded a certain number of coins as an incentive for their effort and resources spent in the mining process.
5. Add new block to the blockchain: The newly created block is validated transactions or smart contracts within it are executed and it is propagated to other peers or nodes. Peers also validate and execute the block. It now becomes part f the blockchain (ledger) and the next block links itself cryptographically back to this block. This link is called a hash pointer.

**BENEFITS OR FEATURES OF BLOCKCHAIN**

1. Decentralization: There is no need for a trusted third party to validate transaction, instead a consensus mechanism is used by nodes to validate and agree on transactions.
2. Transparency and Trust: Blockchains are shared and everyone can see what is on the blockchain network. Blockchain is known as a trustless network.
3. Immutability: Once data has been added to the blockchain it is difficult to change.
4. Highly Secure: All transactions on a blockchain are cryptographically secured and thus provide network integrity.
5. Highly available
6. Cost saving
7. Platform for smart contracts

**LIMITATIONS OF BLOCKCHAIN**

1. Scalability
2. Adoption
3. Regulation
4. Relatively immature technology

**TYPES OF BLOCKCHAIN**

Basically, these are the types of blockchain:

**Public blockchains:** Public blockchains, such as Bitcoin, are large distributed networks that are run through a native cryptocurrency. A *cryptocurrency* is a unique bit of data that that can be traded between two parties. Public

blockchains are open for anyone to participate at any level and have opensource code that their community maintains. Examples are Bitcoin, Ethereum etc.

**Permissioned blockchains:** Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They’re still large and distributed systems that use a native token. Their core code may or may not be open source.

**Private blockchains:** Private blockchains also known as distributed ledger technology (DLT) tend to be smaller and do not utilize a token or cryptocurrency. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information.

NB: There may be other types which have not been discussed here but the ones stated above are the common types. Examples are Hyperledger Fabric, Quorum etc.

**Side-chains**: Side-chains are blockchains connected to the main blockchain, where assets or transactions can be carried in the side-chain and later be recorded in the main-chain. Assets can also eventually be transferred from side-chain to main-chain and vice-versa, and users can send assets to the side-chain so that they can be used there. A good example of a side-chain is the Bitcoin Lightning Network, where Bitcoins can be transacted in a much faster way.

**CONSENSUS MECHANISM**

Consensus is the backbone of a blockchain, as it provides the decentralization of control through an optional process known as mining.

Consensus is a process of achieving agreement between distrusting nodes on the final state of data. To achieve consensus different algorithms are used.

Consensus mechanism is a set of stages that are taken by most or all nodes in a blockchain to agree on a proposed state or value.

**TYPES OF CONSENSUS MECHANISM**

There are several types of consensus mechanisms, but most of them fit into two groups: Byzantine fault-tolerance based and leader-based or proof-based mechanisms.

Byzantine fault-tolerance consensus depends on how nodes are arranged to sign and broadcast transactions. When the majority of nodes agree with what was broadcasted, it can be said that consensus was reached. On the other hand, a leader-based consensus requires the nodes to compete between them in some kind of lottery where they have to guess certain values or take some action like staking coins in order to increase the odds of winning the lottery. The winning node is the one the commits the block to the blockchain. We can see Hyperledger Fabric as a Byzantine fault-tolerant based and Bitcoin and Ethereum as a leader-based consensus.

These are the common used consensus mechanisms:

1. Proof of Work (PoW): It relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network. The miners need to calculate a challenging lottery or mathematical problem in the Bitcoin blockchain and other blockchains using a proof of work consensus mechanism. It’s a bit like trying to guess the number of a lottery ticket. Once a node resolves the lottery, he broadcasts the result to the other nodes, and a new block is appended to the blockchain.

The lottery's difficulty is adjusted to make sure that all the miner's computing power generates one Bitcoin block on average every 10 minutes. Suppose the number of miners or computational power in the network increases, the difficulty of calculating the mathematical problem (aka nonce) will increase to keep the coin distribution/supply and the block production predictable. In that case, proof of work difficulty is adjusted when more people join or leave the network.

In other blockchains such as Ethereum, blocks are added with different frequency. In Ethereum, for example, a new block is added every 15 seconds.

You can see proof of work as a string of data that is difficult to produce (it is time-consuming and resource-intensive) but once discovered, it is easy for others to verify it.

One of the reasons it requires some work to add a new block to the blockchain is to make it more secure. Each miner needs to solve a difficult lottery to add a new block, but if it was too easy, then any hacker could easily try to add new blocks or change the blockchain to his benefit.

The mathematical problem is nothing more than guessing a nonce, a long string of numbers with millions or billions of trial and error. In order words, brute-forcing the result. A miner must guess a nonce, add it to the hash of the current header, rehash the value, and compare the result to the target hash.

The mining difficulty is mostly a measure of how hard it is to find a new block in the blockchain or, in other words, how rare is the nonce is that miners needed to brute force to find a hash smaller than the target hash. In most public/permissionless blockchain, miners will receive a block reward for their work. This reward will likely pay their expenses related to hardware and electricity, and it is an incentive to keep running the network. In 2021, the Bitcoin block reward is 6.25 BTC, and it will continue to be 6.25 until 2024 when it halves again (it halves approximately every 4 years or, to be more accurate, every 210 000 blocks). So in 2024, the Bitcoin block reward will be 3.125 BTC. In 2028 it will be 1.5625 BTC and so on.

1. Proof of Stake (PoS): This algorithm works on the idea that a node has adequate stake in the system that is the node has invested enough in the system so that any malicious attempt by the user would outweigh performing an attack on the network. When creating a new block, the proof of stake algorithm chooses who is the block validator by checking how many coins a person is staking. The bigger the stake, the higher the probability of being chosen as a block validator. In proof of stake, we call the nodes doing the work block validators instead of miners, and we say that block validators mint new blocks instead of mining new blocks.

When a new transaction is issued, it is placed into a block with other transactions, and the block is limited to a certain size in MB. The validating node verifies the transactions' validity in a block and broadcasts the block to the other nodes in the blockchain. After validating the block and sharing it with the other nodes, the validating node will receive a reward if the other nodes agree with the content of the block.

Ethereum is moving to Ethereum 2.0, integrating Casper, a proof of stake consensus mechanism that will switch Ethereum from proof of work to proof of stake. The new Ethereum proof of stake protocol demands block validators to make a security deposit for the validator to be able to participate in the consensus. If they create a fraudulent block, their deposit will be forfeited, and the block validator loses the ability to participate. In proof of stake, block validators increase their chance of being selected to validate a block based on how much do they have at stake. Bigger the stake, the higher the odds of being selected to validate the block and win then reward.

1. Delegated Proof of Stake (DPoS): It is an innovation over standard PoS whereby each node that has a stake in the system can delegate the validation of a transaction to other nodes by voting. DPoS is a consensus mechanism where the stakeholders or hodlers of that cryptocurrency can elect a limited number of validating nodes in an election process. The validating nodes, also called witnesses or block producer in DPoS, validate transactions/blocks and are rewarded for the work.

Typically, elections for the validating nodes are real-time and ongoing, i.e. users/delegates can vote anytime. Stakeholders can vote on who they want to be delegates and block validators/witnesses. The voting power is defined according to the number of coins they own, i.e. more coins translate into more votes (just like a corporation's shareholder voting power). Stakeholders can also delegate their votes to other stakeholders who will vote on their behalf (again, very similar to a corporation shareholder proxy voting). DPoS is, therefore, a democratic process.

Similarly, to proof of stake, block validators receive a reward for validating transactions. They may also be required to have a stake that may be forfeited in case of bad behaviour. Blocks with new transactions can be appended to the blockchain every few minutes. Because DPoS is more centralized in a small number of nodes – EOS, for example, has 21 block producers/witnesses – the network broadcasting is much faster and allows a much better throughput.

If a validating node fails to produce a block or shows some bad behaviour, he can lose his stake and be kicked out of the network. The stakeholders would then vote for a new validating node.

EOS, Steem and BitShares are some of the examples of DPoS blockchains.

Other less consensus mechanisms are:

1. Proof of Elapsed Time (PoET)
2. Proof of Deposit (PoD)
3. Proof of Importance (PoI)
4. Practical Byzantine Fault Tolerance (PBFT)
5. Proof of Activity (PoA)
6. Proof of Capacity (PoC)
7. Proof of Storage
8. Proof of Authority

EXPLANATION OF BYZANTINE FAULT-TOLERANCE

In this problem, a group of army generals who lead different parts of the Byzantine army is planning to attack or retreat from a city. The only way of communicating among them is via a messenger. They need to agree to strike at the same time in order to win. The issue is that one or more generals might be traitors who could send a misleading message. Therefore, there is a need for a viable mechanism that allows for agreement among the generals, even in the presence of the treacherous ones, so that the attack can still take place at the same time. As an analogy for distributed systems, the generals can be considered honest nodes, the traitors as Byzantine nodes (that is, nodes with arbitrary behavior), and the messenger can be thought of as a channel of communication among the generals.

This problem was solved in 1999 by Castro and Liskov who presented the **Practical Byzantine Fault Tolerance** (**PBFT**) algorithm, which solves the consensus problem in the presence of Byzantine faults in asynchronous networks by utilizing the state machine replication protocol. PBFT goes through a number of rounds to eventually reach an agreement between nodes on the proposed value.

PBFT tries to solve the Byzantine General's problem. The Byzantine Generals Problem is a hypothetical situation where a number of generals leading their Byzantine army need to decide if they attack or retreat from the city they are surrounding.

They can only conquer the city if they all attack at the same time and no one retreats. To ensure the operation's success, the Generals need to reach a consensus: they need to wither attack or retreat altogether. They need to communicate horse messengers that carry the information between the generals. One of the problems is that the messenger can be a traitor or be killed halfway. One of the messengers can also change his mind or chicken out, which would compromise the entire army. This is why the Byzantine General's need to have a consensus mechanism to ensure that everyone is on the same page.

In the context of a blockchain network, the potential traitors may be the nodes, and the messengers may be the potentially corrupted communication channels between them. This problem was solved in 1999 by the PBFT algorithm, developed by two computer scientists, Miguel Castro and [Barbara Liskov](https://en.wikipedia.org/wiki/Barbara_Liskov) . PBFT can also be used in other distributed systems other than blockchains, such as peer-to-peer networks and IoT networks.

The PBFT enables decentralized systems to be resilient to failures and allows systems with multiple participants to work in consensus. PBFT systems are resilient, i.e. fault-tolerant, to nodes that are malicious or fail to communicate properly with the other nodes. PBFT can secure systems with multiple nodes and add some resiliency and fault-tolerance.

The Byzantine General's problems:

* The communication channel may not be trusted
* The message could be altered or replaced
* Messenger can be killed
* Messenger can be delayed

The solution:

* Consensus algorithm that it's immune to the lack of trust
* Consensus mechanisms such as PBFT, PoW and PoS are Byzantine Fault Tolerant
* The "good" generals must have more power in the network than the faulty ones
* Cryptography integration to create consensus and data immutability

LINK TO BYZANTINE GENERALS PROBLEM: <https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/>

A **node** can be defined as an individual player in a distributed system. All nodes are capable of sending and receiving messages to and from each other. Nodes can be honest, faulty, or malicious, and they have memory and a processor. A node that exhibits irrational behavior is also known as a Byzantine node after the **Byzantine Generals** problem.

**CRYPTOGRAPHY**

Cryptography is the science of making information secure in the presence of adversaries.

Cryptography is a process defined by data being converted into a certain form so that it is only available to those for whom it was originally intended. However, converted data is inaccessible to an unauthorized end user.

Encryption:

What the process of encryption does is simple. It transforms a particular data into a form that is unreadable. The encrypted data has another common name: Cipher text.

Decryption:

The process of decryption is responsible for converting the unreadable data back into its original form so that it can become readable again. For example, a simple decrypted text, after decryption would become a plain text.

Once data has been encrypted, and it has been sent to the destination of the recipient, there are different ways that can be used for data decryption.

**TYPES OF CRYPTOGRAPHY**

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

Symmetric Key:

Using symmetric keys is easy. When encrypting, as well decrypting, we only use the same keys. An example here would be a door. When you go out to the store, you lock your door using your key, and once you return from the store, you would use the same key to unlock your door right? Well maybe I am wrong; however, typically the same key is used for those purposes.

The symmetric key algorithm is very fast, in fact, thousand times faster than using asymmetric keys. When we were talking about symmetric keys, same keys, they are also called shared secrets. As you can see the problem here is that both the sender as well the receiver must use the same key for both encryption and decryption too. Of course, this is not an advantage when it comes to security, and the blockchain is certainly not using Symmetric key algorithms.

Asymmetric Keys:

Blockchain uses Asymmetric key algorithms as part of other algorithms it uses. Therefore, this topic is what you might have been waiting for.

To implement Asymmetric key algorithm, it requires having two different keys. One of them is called “Public” and the other is called “Private” key. The reason for having two keys is simple. One of the keys will be responsible for encrypting information to become a cypher text, and the other is to decrypt the information to become plain text. The private key would be generated by the originator, the one who would encrypt the information, and this private key must be kept secret at all times. However, the public key would be available to anyone, this is why it’s called the public key.

The asymmetric key algorithm is much slower than a symmetric key algorithm; however, the security is more complex. Therefore, it is harder to be hacked. Both, public and private keys are mathematically interconnected one to another, meaning that each public key has only one corresponding private key. There are few algorithms like that. However, blockchain is correctly using the one called: Elliptic Curve Digital Signature Algorithm.

**BLOCKCHAIN VS. CRYPTOCURRENCIES**

Blockchain started as a cryptocurrency – Bitcoin.

Cryptocurrencies are digital currencies. They rely on the blockchain, but they shouldn't be confused with blockchain. What I mean is that cryptocurrencies always sit on the top of a blockchain, but not all blockchains have a cryptocurrency (Hyperledger blockchains, Corda and other enterprise blockchains are some of the examples of blockchains without cryptocurrency).

Examples of cryptocurrencies are Bitcoin, Ether, USDT etc.

**DOUBLE SPENDING**

Double spending is a type of attack where the attacker attempts to duplicate a transaction. In this attack, the attacker tries to spend the same coins twice, sending it, for example, to a recipient and himself at the same time. Blockchains try to prevent this by time-stamping the transactions and including them in a block. Attackers may try to mine the block that contains the duplicated transaction to increase the probability of tricking the receiver that that transaction was sent.

This kind of attack is more common in proof of work blockchains where the attacker can exploit the intermediate time between two transactions' initiation and confirmation.

Before the second transaction is mined to be invalid (because there is a conflicting first transaction), the attacker already got the first transaction output resulting in double-spending. In this type of attack, the attacker would send the same transaction to a vendors BTC address and a colluding wallet that the attacker himself control. Then, if his transaction gets mined first, he manages to keep the BTC for himself. For this reason, anyone receiving BTC should wait at least for one confirmation, i.e. wait for the transaction to be included in a block. This way, you can make sure that the transaction is settled.

In reality, double-spending attacks require the attacker to gain more than 51% of the network in order to be successful, which is very hard or impossible to happen in any of the major public blockchains. However, the attacker may trick the receiver for a short period of time, and that’s why it is important to wait for a few block confirmations in order to ensure that the transaction was settled in the network.

**MINING**

Mining is the method that is used in the blockchain to group transactions into a block, append this block to the blockchain and broadcast the new block to the network. Mining ensures the consensus mechanism is maintained and keeps the blockchain decentralized.

**WALLETS**

A wallet is used to store a private and public key. It is basically a piece of software that stores the private/public keys and allows the users to sign transactions in order to send a transaction, and allows users to receive transactions using their public key or wallet address.

**BLOCKCHAIN- OUTSIDE OF CURRENCIES**

**Bitcoin**, the first major blockchain conceptualization, was introduced in 2008, it was not until years later that blockchain technology's possible applications in industries other than cryptocurrencies were realized.

These are the major industries blockchain technology can be utilized aside currencies:

* 1. The Internet of Things (IoT)
  2. Government (Voting)
  3. Health
  4. Finance
  5. Media

**THE INTERNET OF THINGS**

IoT can be defined as a network of computationally intelligent physical objects (any objects, such as cars, fridges, and industrial sensors) that are capable of connecting to the internet, sensing real-world events or environments, reacting to those events, collecting relevant data, and communicating this over the internet. After dissecting the definition of IoT, four functions come to light as being performed by an IoT device: **sensing**, **reacting**, **collecting**, and **communicating**. All of these functions are performed by using various components on the IoT device.

Sensing is performed by sensors. Reacting or controlling is performed by actuators; collection is a function of various sensors, and communication is performed by chips that provide network connectivity. One thing to note is that all of these components are accessible and controllable over the internet, via the IoT. An IoT device on its own is useful to some extent, but if it is part of a broader IoT ecosystem, it is more valuable.

**GOVERNMENT**

There are various applications of blockchain being researched currently that can support government functions and take the current model of e-government to the next level.

Government, or electronic government, is a paradigm where information and communication technology are used to deliver public services to citizens. The concept is not new and has been implemented in various countries around the world, but with blockchain, a new avenue of exploration has opened up. Many governments are researching the possibility of using blockchain technology for managing and delivering public services, including, but not limited to, identity cards, driving licenses, secure data sharing among various government departments, and contract management. Transparency, auditability, and integrity are attributes of blockchain that can go a long way in effectively managing various government functions.

**HEALTH**

In healthcare, major issues such as privacy compromises, data breaches, high costs, and fraud can arise from a lack of interoperability, overly complex processes, transparency, auditability, and control. Another burning issue is counterfeit medicines; especially in developing countries, this is a major cause of concern.

With the adaptability of blockchain in the health sector, several benefits can be realized, including cost savings, increased trust, the faster processing of claims, high availability, no operational errors due to complexity in the operational procedures, and preventing the distribution of counterfeit medicines.

**FINANCE**

Blockchain has many potential applications in the finance industry. Blockchain in finance is currently the hottest topic in the industry, and major banks and financial organizations are researching to find ways to adopt blockchain technology, primarily due to its highly desired potential to cost-save.

These applications include, but are not limited to, insurance, post-trade settlements, financial crime prevention, and payments.