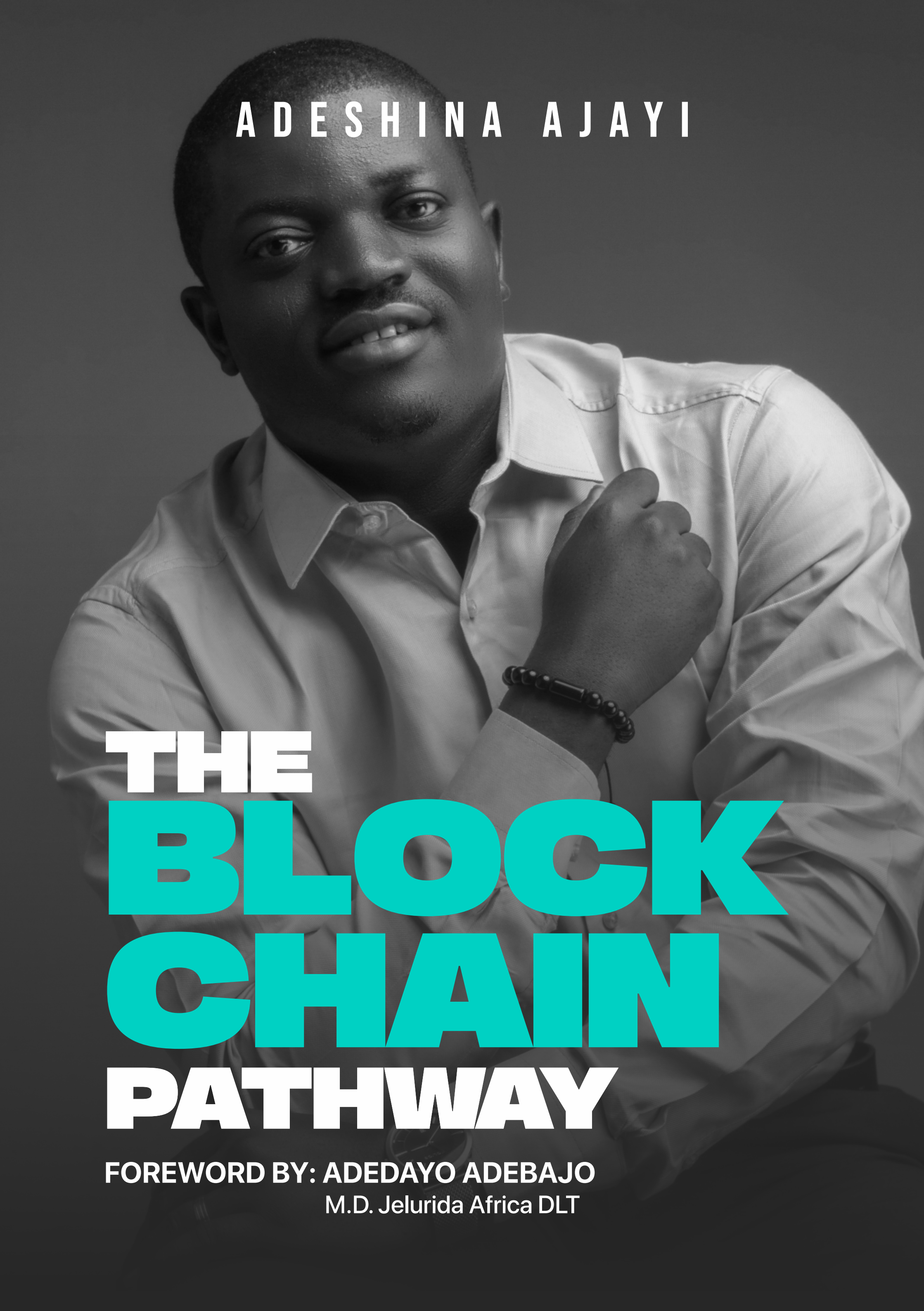

ADESHINA AJAYI

THE BLOCKCHAIN PATHWAY

FOREWORD BY: ADEDAYO ADEBAJO
M.D. Jelurida Africa DLT

ADESHINA AJAYI

BEST SELLING AUTHOR
OF **WEALTH TRANSFER**

THE BLOCKCHAIN PATHWAY

ADESHINA AJAYI

DIGITAL FOCUS

PUBLISHED BY:

ACE world Publishers

Magazine: Opportunities, Education, Career

For information, NIGERIA; Plot 7, Close A, Adfarm Estate, Alakuko, Lagos.

Adeshina Ajayi's books may be purchased for educational, business, or sales Promotional use. For more information, please e-mail; ajayiadeshina5@gmail.com

ISBN: 978-978-995-906-8

TABLE OF CONTENTS

PART II: THE BLOCKCHAIN ECOSYSTEM

PART III: INTRODUCING SMART CONTRACTS

PART IV: CRYPTOGRAPHY

Acknowledgements

My first debt is to God for life.

To my beautiful family, the gift of you is everything. Adedayo my wife, Brian and Ethan my sons. You all make purposeful living an easy ride. Thank you.

A big thank you to every member of my team at Digital Focus. Sam, Treasure, Tomi, Emmanuel, Shelle, Atarashe, Femi. You're the best any leader could ask for. Your contributions are highly appreciated,

ACE World Publishers came through as always. Special thanks to the team for the great job they did.

To my dear brother and friend, Emmanuel Smart. Thank you for being an inspiration always.

I can’t but appreciate my industry leader, Mr Adedayo Adebajo MD Jelurida Africa DLT. Thank you for all the time, efforts and resources you’re putting in to the growth and development of blockchain in Africa. Thank you for writing the foreword of this book. It’s a privilege I do not take for granted.

Blockchain council filled a huge knowledge gap on blockchain subject matters. Thank you.

And to you dear reader, thank you for making the choice to read this book. I hope it is worth all the time and resources invested into it.

Thank you.

Foreword

It gives me great pleasure to write this foreword for many reasons, part of which is that I believe in the value of educating people on distributed ledger technology and its importance in fostering fast adoption of decentralized solutions especially in Africa. Events do come and go, but a book stays and becomes a reference point to learn more. The application of the technology in the public and private sectors is just the liberating element Africa needs and perhaps some have been waiting for.

There is a lot of untapped resources in the decentralized and digital world. But these resources will remain untapped if people are not informed on their existence. Blockchain technology is one of such emerging technologies that offers to liberate many businesses, creates new models, and make Africa great. The level of transparency and security offered by the technology induces trust even in unknown parties paving ways for various transactions to flow through the distributed ledger. These transactions can include financial transactions among other digital assets transacted peer to peer between parties in the virtual world.

Asides from the single point of failure of centralized systems in the incidence of a cyberattack also comes the lack of trust in systems that allows an Admin to manipulate data because of the privilege provided. Unwarranted trusts and office privileges today aren't even the only thing wrong with centralized systems. The big giant companies applying user data as traffic to earn income in billions, the pharma research using patients' data to create/validate new products for personal profit and so on. Data is said to be the new gold but people are less informed on how that works. These data are applied by many companies with no dime paid to the owners of the data. Decentralized systems being distributed are not only secure and immutable but provides incentives for data sharing.

This book provides numerous valuable information suitable for techy and non-techy people interested in learning about the technology of the future today. It provides instances of each application with samples on various industries where it is being applied and areas it can further be applied. A lot of people have questions on these emerging technologies and how they can plug into it but with no idea on who to ask. Another big challenge we currently face is the attribution of blockchain technology to mean only cryptocurrency. To encourage adoption of the technology, a lot of people need to be educated and that is one of the purposes this book stands to serve.

Adedayo Adebajo,

M.D. Jelurida Africa DLT.

Introduction

Blockchain technology was initially applied solely in cryptocurrency transactions such as bitcoins; however, with the rise of blockchain-based applications, the potential benefits of this ground-breaking technology are unparalleled.

It is worthy to note however, that blockchain is a disruptive technology, hence, it is essential that effective planning and research is done before applying blockchain to different sectors of the African economy.

Governments of developing economies like Africa also need to stimulate entrepreneurial awareness of emerging technology through training and promotion to facilitate investment readiness.

Similar to every emerging technology, the adoption of blockchain to its full potential is dependent on the extent to which relevant stakeholders take the lead in supporting and unveiling market-creating innovations in blockchain platforms.

This book explains how blockchain is being applied across various industries in the world, and how Africa, particularly Nigeria, can use it to increase efficiency and transparency.

CHAPTER 1:

WHAT IS BLOCKCHAIN?

Many people confuse blockchain with cryptocurrencies—Bitcoin in particular. So let's clear this misconception right away: Blockchain is not a cryptocurrency. Blockchain is the technology behind cryptocurrency, and this is just one use-case of the technology. Blockchain is a platform that makes certain applications possible, just like an Operating System makes it possible to edit text or create a design of graphic nature.

Think of how you are able to create and edit text on your laptop or smartphone, or how you can create designs of graphic nature using tools specifically geared toward such applications. These applications exist because of the Operating System (OS) that are housed in such devices.

This is exactly how blockchain functions: It is like an OS providing a platform for many possibilities, and Bitcoin is just one of its many applications. Just that while an OS is a housing for utility applications, Blockchain is more inclined to transactional and record-keeping applications.

****

Blockchain is a decentralized ledger that tracks digital assets on a Peer-to-Peer network. On this network, each node (computer/server) is connected to all the others in some way, and each node holds a copy of the ledger.

Think of it as a bank statement. For example, you and four other friends hold a copy of this same statement. When any of your friends make a transaction, the system will check the last statement to determine if it is the same in all the other four. Only once this background check is completed and approved can a new transaction take place. After the transaction is completed, it will be updated in all five ledgers. If anybody tries to manipulate their statement, it won’t match the rest of the ledgers. This is a sure-shot way of avoiding fraud. Now, imagine this happening on thousands of machines for every transaction. An attacker cannot manipulate so many devices simultaneously.

A BOOK ANALOGY

In a typical bookcase, each page in the book contains some data. Think of the book as the blockchain; every individual page as a single block, and the data on each page as a blockchain transaction. All these pages are in a particular order and contain references to previous pages.

If any page is removed or deleted, it is easily identifiable because each page is numbered. Removing one page will affect the entire ledger. For example, if you remove page 65 from a 100-page book, it will get noticed when somebody tallies it.

Now, if fifty friends have the same copy of this book in their possession, one person that has a page missing from her book can easily refer to the copy in possession of any of the other forty-nine for the missing page's contents.

This is precisely what makes blockchain so transparent and reliable: because everything is recorded in thousands of places at once, no one can tamper with it. A digital asset or currency is just a number defined in a blockchain carrying some value. It could be an apple, a chair, or a book. It just has to be of value for the two parties involved in a transaction. For example, Bitcoin is only a number stored in the ledger and tracked from day zero, but with its popularity, it has gained value.

DATABASE, THE ROOT OF BLOCKCHAIN

Blockchain technology is, at its fundamental level, a database structure; a system for storing information electronically. Let's use an illustration to better understand.

Think of a school, for instance. The average school has hundreds of students in its system, and each student must be fully accounted for if the school's education system and overall program are to be run effectively. Details such as the year of entry, age, gender, and the class of each student must be recorded and updated regularly.

Imagine putting all that information on paper. While it is not impossible, creating and maintaining such a huge collection of information in this manner will surely prove to be quite tasking, not to mention the tediousness—and frustration—one would experience trying to create copies for different personnel to be able to access it as the need arises.

But when such information is stored electronically (in a computer system for instance), updating and making it accessible to others instantly becomes quite easy.

This is what a blockchain is: a database for storing information structurally.

But databases have been existent for decades now, so what makes this one any different or special?

WHAT MAKES BLOCKCHAIN UNIQUE

Many things make blockchain unique, but three major features clearly distinguish it from its counterparts:

1. Its method of storing information
2. Its decentralized form of management, and
3. Its immutability.

1. STORAGE

While database systems commonly store their information in tables and sheets, this one stores information differently: in blocks.

A blockchain involves a network of computers with an established peer–to–peer connection. These computers are known as nodes.

Whenever a transaction is initiated within the network, the transaction request is broadcast to all the computer systems to verify it. The transaction is validated, and a reference code called a "hash value" is generated. This value is linked to the details of the completed transaction and clustered with the hash values of other transactions, creating a block of transaction details.

Now, blocks possess certain storage capacities. So when a block is filled, it is chained onto the previously filled block. As new transactions are executed, new blocks are created and linked together, forming a "chain of blocks." This is what has come to be called the blockchain system as we know it today.

“Blockchain relies on distributed ledger technology (DLT)[1]. The DLT acts as a decentralized database of information about transactions between various parties.

Operations fill the DLT in chronological order and are stored in the ledger as a series of blocks. An interconnected chain is formed between blocks with each one referring to the block before it, thus creating a blockchain.

“In blockchain storage, files are first broken apart in a process called sharding[2]. Each shard is copied to prevent loss of data should an error occur during transmission.

The files are also encrypted with a private key that makes it impossible for it to be viewed by other nodes in the network. The replicated shards are distributed among decentralized nodes all over the world."

"The interactions are recorded in the blockchain ledger, allowing the system to confirm and synchronize the transactions across the nodes in the blockchain. Blockchain storage is designed to save these interactions forever and the data can never be changed." (Forbes, 2021)

Blockchain storage vs. cloud storage

Blockchain storage is a potentially cheaper, more secure and more reliable alternative to centralized cloud storage.

Providers of centralized cloud storage prevent data loss by making copies of the data and storing it in different data centers. The large amount of data that is duplicated in this process can create excessive amounts of surplus information.

Also, cloud storage requires enterprise-grade hardware for its data centers. These factors can make centralized data storage significantly more expensive than blockchain storage. (Gbksoft, 2021).

2. DECENTRALIZATION

This is one of the things that makes blockchains special. A typical database is usually found in one location, housed in one computer or a group of computer systems that make up its local server, and all of its information is controlled by one person or a group of people. They make up a central authority that exercises total control over all the information stored within the network—including its update and maintenance. Whatever they want it to be, is what it is.

Recalling the example of the school database, if, for instance, a lecturer wishes to unduly favour a student who performed poorly in their exam, the lecturer simply needs to input the 'preferred' score into the student's score sheet, and the entire public (other students and teachers) would be none the wiser.

This is how a conventional database is run; a specific individual or group wielding complete influence over all its information, acting as a central authority determines what is true and what is false. Brings to mind the 'Big-Brother' concept: Everything is contained within their scope of observation and influence.

With blockchain, it's a different game altogether. Except for privately owned and operated systems, blockchains are typically decentralized: i.e there is no central authority controlling the blockchain's database. Also, the network of computer systems that make up the servers for its database are dispersed across different locations, and every participant of that network wields equal access to—and control of—its information. This makes it so that no one component can alter or manipulate any portion of data without the involvement and approval of all the others, making it practically impossible to hack, cheat, or tamper with the blockchain database.

HOW DOES DECENTRALIZATION WORK?

To understand this vital aspect of blockchain even better, let's examine how it has been implemented by Bitcoin. Like any database, Bitcoin needs a collection of computers to store its blockchain. The blockchain in this case is simply a specific type of database that stores every Bitcoin transaction that is ever made. Just as we learned earlier, these computers are not all under one roof, and each computer (or group of computers) is operated by a unique individual or group of individuals.

Now, imagine this: A company owns a server powered by 12,000 computers, and this server houses a database of all of its clients' account information. All the computers are placed together in a warehouse, and the company of course has full control of every one of these computers and the information contained within them. In comparison, Bitcoin also consists of thousands of computers, but each computer or group of computers holding its blockchain is in a different geographic location, and the computers are not operated by one person, but by separate individuals or groups of people. These computers that make up Bitcoin’s network are called nodes.

This is how Bitcoin’s blockchain is used in a decentralized way. However, there are privately owned, centralized blockchains where the computers that make up its network are owned and operated by a single entity.

In a blockchain, every node possesses a full record of the data that has been stored on the blockchain since its inception. For Bitcoin, this data is the entire history of all Bitcoin transactions. If one node should have an error in its data, the thousands of other nodes will act as a reference point for correcting it. As a result, no single node within the network can alter information held within it. Consequently, the history of transactions in each block that makes up Bitcoin’s blockchain is irreversible.

So if one user tries to manipulate any portion of Bitcoin’s record of transactions, all the other nodes would compare records with one another and single out the node with the inconsistent information. This data is then dismissed as incorrect, and replaced by the 'correct one. This system helps to establish an exact and transparent order of events. In Bitcoin's blockchain, the information is a list of transactions, but blockchain's storage is not limited to transactional information; it is also useful for information like legal contracts, state identifications, or a company’s product inventory.

For any portion of the information stored within a blockchain to be changed, a majority of the decentralized network’s computing power must first agree on such a change. This ensures that whatever change does occur is in the best interests of the majority.

A Forbes article by Roomy Khan highlights many benefits and developmental opportunities that decentralization has brought along with it.

“Decentralized networks, Cryptocurrencies, Non-Fungible Tokens (NFTs), Blockchain, Bitcoin, Ethereum, DIFINITY, etc., are incessant buzzwords in the media.

“However, behind the hype, numerous palpable applications are being developed using distributed ledger technologies like blockchain, which are expected to unleash new markets and operating business models; displacing the grip of the current near-monopolistic centralized businesses.

“Internet behemoths like Amazon, Google, Facebook, Twitter, etc., are centralized aggregator- distributor platforms that collect, own, analyze, and monetize user data through targeted advertising, selling products and services.

“Their scale and near-zero marginal cost allow them to provision their platform services to the farthest reaches of the globe. Colossal ever-growing centralized repositories of data give them an asymmetrical advantage through ‘winner-take-all’ benefits and near monopolistic power to garner superlative profits; and even control the social discourse and narratives.

“Most aggregator-distributor platforms get the user data for free, handsomely profiting from it, and have exclusive access and usage rights. In return, they deliver egalitarian experiences globally, resulting in exponential consumer/user acquisition through network effects.

“In the incumbent centralized internet-based consumer market value chain, aggregators-distributors entrenched between the upstream suppliers and the downstream consumers/users pocket most of the money.

“For Q1, 2021, Amazon reported a profit of $8.1 billion; Google reported a profit of $17.9 billion; Facebook reported a profit of $9.5 billion; Twitter reported a profit of $68 million.

“Decentralized applications (dapps) such as payment rails, DeFis, NFTs, etc., acting as supporting services to the decentralized talent networks, can bring paradigm-shifting efficiencies and economic opportunities for all participants.

“For example, payment rails can allow users to make P2P cross-border payments. Likewise, DeFi capabilities, including lending, borrowing, trading, and staking, can enable users to get supplemental economic benefits.

“Braintrust, a blockchain-based digital talent freelancer, connects technical and design freelancers with US companies via a bidding mechanism. When companies using the platform hire freelancers, they pay Braintrust 10% of the bid amount as a fee.

“Bondex, a decentralized talent ecosystem, is built on a global professional network powered by AI and utilizing blockchain. Company will add services for network participants by drip releasing decentralized applications (dapps), such as payments rails and DeFi capabilities, etc.

“In addition, the company will share a portion of its revenue as a financial reward for participating and vesting in the ecosystem. "At Bondex, our users are not the product. They are real stakeholders in the growth and success of the talent ecosystem through tokenized revenue sharing mechanisms," said Ignacio Palomera, Bondex Chief Strategy Officer.

“Unlike the contemporary solutions and business models, Bondex's reward system uniquely provides economic opportunities to its ecosystem participants.

“Through rich global P2P interactions, blockchain and crypto technology applications are ready to disrupt the talent markets and address the needs of the gig economy in the post-pandemic world.” (Forbes, 2021)

3. IMMUTABILITY

Blockchain's information is immutable, that is, once data is entered, it is permanent; cannot be reversed. This, along with decentralization, makes Blockchain's structure a major break away from the typical database system.

If blockchain technology were to be implemented in our illustrative school system, exams would be organized such that a network of computer systems with pre-programmed automation would be the ones to receive the students' answers, compare them with the answers already provided as correct and permanently store the score for the students, making it impossible for records to be manipulated.

Data stored on the blockchain cannot be altered. Each block of information, such as facts or transaction details, proceeds using a cryptographic principle or a hash value. That hash value consists of an alphanumeric string generated by each block separately.

Every block not only contains a hash or digital signature for itself but also for the previous one. This ensures that blocks are retroactively coupled together and unrelenting. This functionality of blockchain technology ensures that no one can intrude in the system or alter the data saved to the block.

It is also important to know that blockchains are decentralized and distributed in nature, where a consensus is made among the various nodes that store the replica of data.

This consensus ensures that the originality of data must be maintained. Undoubtedly, immutability is a definitive feature of this technology. This concept has the ability to redefine the overall data auditing process and makes it more efficient, cost-effective, and brings more trust and integrity to the data.

A post by DZone outlines the challenges that have popped up with immutability, as well as their proposed solutions.

How Immutability Is Achieved

“As explained above, the hash value secures each block of code separately. Though, the point of interest is how it establishes immutability. To comprehend this scenario, you need to understand cryptographic hashing.

Cryptographic Hash Basics

“Today, generating a cryptograph isn't dreadful, as modern programming languages are provided with several "hash functions." With these, one simply needs to pass a set of bytes and the function will return a checksum signature.

“There is no dearth of functions under this umbrella; however, the SHA-256 is popular in the blockchain space. Let's better understand with an example.

“For instance, you want to generate a cryptographic hash in Python code. For this, you need to import the hashlib package from the standard library of Python, which offers access to the sha256 function. Let's look at the code.

“These functions are generating a string of 64 characters. Irrespective of the size of the input, you will always get the same fixed length of the string, which is known as the digital signature.

“This digital signature points to the exact data that you input. The key utility of this hash that you can't reverse-engineer it. It means you will not be able to use this output string to find the input data. It simply results in immutability.

Cryptography + Blockchain Hashing Process = Immutability

“In this system, transactions verified by a blockchain network include blocks of information embedded with timestamps, which is secured by a hashing process. It links together and incorporates the hash of the previous block. This mechanism develops the chronological chain that joins each block.

“The hashing always includes the meta-data of the previous block while generating a new hash for it, which establishes a link between the block and the chain then becomes " unbreakable." After this, nobody can delete and alter the data of the block placed in the blockchain, because if somebody attempts this, the subsequent block rejects the modification (as the hash of block wouldn't be valid anymore).

“It is true that this is a robust mechanism. However, there are several challenges that this mechanism has to overcome.

Challenges to Immutability of Blockchain

51 Percent Attack

"There are a number of challenges for this mechanism. However, the chief weakness can be the possibility of a "51 percent attack." What is this? Well, this term signifies that an attacker can acquire huge computing power over all other members of the network. In short, it can be referred to as "controlling interest in generating power."

"As I mentioned above, it is a decentralized form of a network where no single entity is in charge. Yet, miners together can spell death for the immutability of the blockchain system by just creating a majority of hashing power. Now, owing to the upsurge in mining marketplaces and the accessibility to renting mining capacity, there is no difficulty for people to carry out such an attack.

“This allows attackers to alter the transaction data that is supposed to be "immutable" first. With this facility, attackers can reverse the high-value transaction, spend the money the second time, and secure the profit.

Quantum Computing

“Another big challenge in this space is quantum computing, which is threatening blockchain's trait of immutability. Experts at IBM have asserted that quantum computing has the ability to reverse-engineer the public key of the blockchain network, which can find the private keys to break the system. There is no doubt in saying that this is a real and credible threat in the space, which is capable of affecting almost 50 percent of blockchains.

Solution

“Experts suggest that the “51 percent attack” can be tackled by creating a stronger protocol and by using a consensus algorithm such as delegated proof-of-stake” or just “proof-of-stake” algorithm.

“Why is this needed? Well, it is hard to stake numbers of tokens on a network instead of renting out computing power. Though, it is hard to say that these solutions are reliable enough in such a threat.

“For the threat of quantum computing, many application developers have recommended integration of quantum cryptography into the core of blockchain. In the upcoming years, the blockchain architecture created with quantum particles will be able to record all history in a more secure way.

“The solutions to these are quite futuristic. So, for now, be mindful of adopting blockchain and the benefits available to create robust application solutions.” (DZone, 2019)

CHAPTER SUMMARY

- A blockchain is a decentralized ledger, tracking digital assets on a Peer-to-Peer network.

- A blockchain's network consist of many nodes, which are computer systems acting both as storage locations and servers for the network.

- Three things make Blockchain technology stand out from other typical database systems:
  - Its method of storing information
  - Its decentralized form of management, and
  - Its immutability.

- Blockchain storage, by virtue of its nature, is significantly more efficient than centralized cloud storage.

- Decentralization in blockchain network means that data is available to, and accessible by, everyone.

- Every transaction record on the blockchain network is impossible to change or delete once written, making it by extension impossible for anyone to tamper with any of them without first controlling the majority of the network first. This amazing level of security has made blockchain an exceptional digital vault for information storage.

- People are currently finding ways to skirt around the immutability of blockchain networks, and experts are working on solutions to this new threat.

CITATIONS

1. Khan R. (2021, June 27). *Decentralized Blockchain Networks Are Getting Ready To Disrupt Talent Markets*. Forbes. https://www.forbes.com/sites/roomykhan/2021/06/27/decentralized-blockchain-networks-are-getting-ready-to-disrupt-talent-markets/?sh=5f11fda47612

2. Anna, Ksenjija. (2021, July 16). *Blockchain vs Cloud Computing: Best Features for Corporate Space*. Gbksoft. https://gbksoft.com/blog/blockchain-vs-cloud-best-features-for-corporate-space/

3. Srivastav, K. (2019, March 29). *A Guide to Blockchain Immutability and Challenges*. DZone. https://dzone.com/articles/a-guide-to-blockchain-immutability-and-chief-chal

CHAPTER 2:

COMPONENTS OF A BLOCKCHAIN

Each block in the blockchain is created and established by a protocol of computations, which we shall now inspect closely. Learning about their roles to play in the formation of new blocks will help us understand the whole concept of the blockchain even better.

Every block consists of two major segments: the block header and the block body.

THE BLOCK HEADER

This segment houses six components laden with the information that propels the entire blockchain structure. Let’s go through them:

I. Version Number: This describes how the current block's data is structured, enabling computers to read the content of the block correctly.

II. Previous block hash: A hash is a string of characters that is formed when sets of data are merged as one. The sets of data in this context are the details of different transactions performed in the blockchain network. These details are merged through a computational process called hashing; hence the name given to its resulting value. Every block has a hash that links it to the block before it. This hash is the chain linking all the blocks together in a chronological manner. It contains the hash of the previous or parent block.

III. Merkle Root: Or the “Root Hash”. It is the value representing the Merkle Tree: more on this when we get to the body of the block.

IV. Timestamp: The time of the current block is calculated in seconds since the first second of the first day of January, 1970. This value is recorded in the block.

V. Goal: Or Target, a numerical value that miners work with to validate a block so they can add it to the blockchain. It represents the difficulty of adding a new block to the blockchain system.

VI. Nonce: Nonce is an abbreviation for “number only used once”. It’s a variable that is hashed repeatedly with the Goal/Target value mentioned earlier, with the intent of finding a value that is lower than the Target.

THE BLOCK BODY

If the blockhead is the front segment of a lorry consisting of the engine and other gears—as well as the particulars in the cockpit detailing the purpose of the vehicle, then the block body is the flatbed with all its luggage: the transaction details contained in the block.

Just as its likening example, the transaction details are not just packed and dumped onto the block, but are bundled and into packages and stacked together by hashing them to form a Merkle Tree.

The Merkle Tree derives its name from its founder, Ralph Merkle, who discovered that much information could be represented in a single line of text. The details of each transaction in a block (an average of 500) are integrated to form a hash (Merkle leaves), which are then paired with other hashes—and then hashed again (branches), and merged to form a Tree. This tree is situated in the body of the block. Finally, the tree itself is hashed until a single hash is arrived at (the Merkle Root).

CHAPTER SUMMARY

- Every block on a blockchain network consists of two major segments
  - the block header, containing the version number, previous hash, timestamp, goal and nonce.
  - the block body, which contains the Merkle Root.

CHAPTER 3:

BLOCKCHAIN HISTORY: HOW IT ALL STARTED

In 2008, a white paper was released by an entity operating under the pseudonym Satoshi Nakamoto. Nakamoto spoke of creating 'Bitcoin' as a form of cash that could be sent peer-to-peer without the need for a central bank or other authority to operate and maintain the ledger.

Blockchain is the engineering framework through which Bitcoin was implemented.

HISTORY OF BLOCKCHAIN

Blockchain technology might seem like rocket science, and many would naturally be inclined to believe the technology was rolled out very recently. Taking a closer look, however, will reveal an entirely different situation: the blockchain concept has been in existence for many years—well over a decade now.

EARLY YEARS

In the year 1982, cryptographer David Chaum was the first to propose something similar to a blockchain protocol in his dissertation titled *"Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."*

Indeed, blockchain technology began to pick up speed in 2008. But the groundwork for what we have today was first laid by Stuart Haber and Scott Stornetta in 1991. They intended to implement a system where document timestamps could not be altered. Their system utilized a cryptographically secured chain of blocks to store said documents. Then in 1992, the Merkle Tree data structure was incorporated into the framework, ensuring that the system became more efficient and enabling the collection of different documents into a single block. This invention, unfortunately, never saw the light of day.

The anonymous Satoshi Nakamoto (who could either have been a group of people or an individual) is accredited as the brains behind blockchain technology, as he created the first workable application of the technology which was initially confined within the financial landscape in 2009.

Transaction Phase (Emergence of Bitcoin)

There are a lot of people who use the terms "bitcoin" and "blockchain" interchangeably. In other words, they believe both are the same. Howbeit, this is not the case, as one is the technology powering several applications of which cryptocurrency (Bitcoin) happens to be one.

Bitcoin came into existence on the 3rd of January, 2009, with the first block being mined by Satoshi Nakamoto. This first application of blockchain technology was designed to be an electronic peer-to-peer system facilitating the seamless transfer of value.

Smart Contracts (Ethereum development)

For a technology still in its formative years, we were bound to see one major innovation right on the heel of another.

Vitalik Buterin ensured that we did not have to wait long as he rolled out the Ethereum blockchain, which was intended to fully leverage the capabilities of blockchain technology by adding functions well beyond the peer-to-peer, cryptocurrency nature of Bitcoin. He introduced "smart contracts'', an application with the ability to credibly effect the negotiation of a contract—and by so doing, completely taking out the influence of third parties.

There will be more explanations on the intricacies of smart contracts in subsequent chapters.

CHAPTER SUMMARY

- Blockchain is the engineering framework through which Bitcoin was implemented.

- Blockchain development began as far back as 1982, and over time, different people created innovations that served to be the different components making up the features it now possesses.

- Bitcoin, the mother of cryptocurrency, came onto the scene on the 3rd of January, 2009.

- Vitalik Buterin rolled out the next big thing about blockchain network with the Ethereum blockchain.

CHAPTER 4:

THE IMPACT OF BLOCKCHAIN IN OUR WORLD TODAY

Blockchain technology has been in existence for a little over a decade now, and yet, is still considered to be in its infancy. This is because the world is largely unhurried to fully embrace this highly disruptive innovation that has carved a distinct signature for itself in the technology field. In a nutshell, we're all still trying to "get used to it".

Still, blockchain has made a definite impact in our world, and the majority would agree that this novel innovation is here to stay.

Let us explore some of the ways in which blockchain has successfully weaved itself into the fabric of things today.

Finance

The finance industry has seen the most action from blockchain, as its first known implementation is financial. The creation of Bitcoin and other cryptocurrency assets has ushered a new season into the world of finance, where transactions are now sped up without the need to involve third parties in their verification processes.

"Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.

"By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely."[1] (Investopedia, 2020).

Very recently, I needed to make a cross-country transaction involving thousands of dollars, and when I contrasted how much I would pay in fees between bank transfer and crypto transfer, I discovered that I would be charged a fee of $228 to make the transaction by bank-transfer, and it would take hours (if not days) for the money to arrive at the recipient's end.

If, however, I were to buy USDT of the same value with the amount of money I wanted to send, I would be charged a fee of 1USDT; the equivalent of $1 to send it out. And the money would hit the recipient's wallet in 10 minutes at the most. Just consider that vast difference!

These are just a few instances of the impact that blockchain technology has made in the finance sector.

The following case study from cbinsights shows us just how much of an impact blockchain has made on finance.

“Today, trillions of dollars slosh around the world via an antiquated system of slow payments and added fees.

“Facilitating payments is highly profitable for banks, providing them with little incentive to lower fees. For instance, cross-border transactions, from payments to letters of credit, generated $224B in payments revenues in 2019.

“Cryptocurrencies like bitcoin and ether are built on public blockchains (Bitcoin and Ethereum, respectively) that anyone can use to send and receive money. In this way, public blockchains cut down on the need for trusted third parties to verify transactions and give people around the world access to fast, cheap, and borderless payments.

“Bitcoin transactions take 10 minutes on average to settle, although this can lengthen to hours or even days in extreme cases. That’s still not perfect, but it represents a leg up from the average 3-day processing time for bank transfers.

“And due to their decentralized and complex nature, crypto-based transactions are difficult for governments and regulatory bodies to control, observe, and shut down.

“Developers are also working on scaling cheaper solutions to process crypto transactions more quickly. Bitcoin Cash and TRON, for example, have relatively low-priced transactions.

Examples of improved payments through blockchain

“While cryptocurrencies are a long way from completely replacing fiat currencies (like the US dollar) when it comes to payments, the last couple of years have seen mostly upward growth in transaction volume for cryptocurrencies like bitcoin and ether. In fact, the Ethereum network became the first to settle $1T in transactions in one calendar year in 2020.

“Some companies are using blockchain technology to improve B2B payments in developing economies. One example is BitPesa, which facilitates blockchain-based payments in countries like Kenya, Nigeria, and Uganda. The company has processed millions of dollars in transactions, reportedly growing 20% month-over-month.

“BitPesa is also widely used for remittances sent throughout sub-Saharan Africa, the most expensive region in the world for sending money. Crypto payments platforms such as BitPesa have led to a reduction of over 90% in transfer fees in the region.

“Blockchain companies are also focusing on enabling businesses to be able to accept cryptocurrencies as payment. For example, BitPay, a payment service provider that helps merchants accept and store bitcoin payments, has a number of integrations with e-commerce platforms like Shopify and WooCommerce.

“Ethereum-based payments platform Airfox, which was acquired by Brazil-based retailer Via Varejo in May 2020, has partnered with MasterCard to allow customers to pay using its banQi app at global points of sale, as well as at every Via Varejo location.

“HUPAYX, a South Korea-based crypto payments startup, partnered with several South Korean businesses in 2019 to create a payments network. Consumers in the country can now pay using the HUPAYX mobile app and point-of-sale infrastructure at over 400,000 stores, including duty-free stores and shopping complexes.

“Blockchain technology is also being used to facilitate micropayments, which represent amounts usually less than a dollar. For instance, SatoshiPay, an online cryptocurrency wallet, allows users to pay tiny amounts to access paid online content on a pay-per-view basis. Users can load their wallet with bitcoin, US dollars, or any other payment token supported by the app.

“One big reason behind the coming disruption of the payments industry is the fact that the infrastructure supporting it is just as liable to disruption — the world of clearance and settlements.” -- (CBINSIGHTS, 2021).

Intensified Research

In the advent of blockchain technology, many companies and entities have embarked on intensive research to discover new ways in which blockchain can be implemented—especially since the discovery that while blockchain's first successful implementation was financial, it could also be applicable in other industries like healthcare, chain supply, and property tracking.

Companies like Amazon, Microsoft, Deloitte, among others are currently working on how they can integrate blockchain into their services in the nearest possible future.

The burden of manual processes

“Most supply chains rely heavily on manual processes, making it difficult and time-consuming to trace back an issue, such as the E.coli romaine lettuce problem from last spring, responsible for at least 200 getting sick. Each year worldwide, unsafe food causes 600 million cases of foodborne diseases. To trace back the source, it can take up to a few weeks. Being able to trace the origin of food could not only allow companies to act quicker when a contaminated food source is identified but could ultimately help save lives.

“Enterprises get overwhelmed by vast amounts of information coming from suppliers and customers in varying locations, from pricing to labor agreements to tax documents and more. There are simply not enough hours or people to complete carry out the processes quickly and error-free.

“While many businesses view a fully digital supply chain as a pipe dream, they can start their journey through small and non-intimidating pilots. Those who take the first step see the organisational payoff quickly.

Introducing Blockchain to food supply chain

“Walmart has been working with IBM on a food safety blockchain solution to add transparency to the decentralised food supply ecosystem by digitising the food supply chain process. They created a food traceability system based on Hyperledger Fabric, the open-source ledger technology. By placing a supply chain on the Blockchain, it allows making the process more transparent and traceable. Each node on the Blockchain represents an entity that has handled the food on the way to the store, making it a lot easier and faster to see if one of the farms has sold an infected batch to a specific location.

“The team at Walmart co-led the core design and setup of the application with IBM as well as built the integration with the enterprise systems. They worked with the standards authority in barcodes and labelling to define the data attributes for upload to the Blockchain. IBM then wrote the chain code. Suppliers used new labels and uploaded their data through a web-based interface.

“Together with Walmart, IBM ran two proof of concept projects to test the system. One focused on tracing back mangos sold in Walmart’s US stores, and the other looked at the sources of pork sold in China. In both cases, the system has proven effective. In China, the system was used to upload the certificates proving the authenticity of the pork to the Blockchain, something considered impossible before. In the US, it typically took approximately seven days to trace the origin of mangoes. That time has been reduced to 2.2 seconds. The good news is, to benefit from the system, suppliers don’t have to be blockchain experts by any means. They just have to know how to upload data to the blockchain application.

“Below timeline illustrates the process of development:

Broader implementation

“IBM also is already implementing blockchain tech in healthcare systems to provide transparency and integrity of data, as well as exploring how they can provide a network for easy exchange and management of skills-based credentials.” -- (The Leadership Network, 2020).

INCREASED CONSCIOUSNESS OF TECHNOLOGICAL RELEVANCE

Technology has successfully weaved itself into the fabric of our daily living, and with every new discovery to its practical application to problem solving, technology is becoming more and more indispensable.

The introduction of blockchain technology further proves this. As more and more investment is poured into research on ways in which this technology can be practically employed, there is a notable spike in people's awareness of—and interest in—the technology's increasing relevance.

People are realizing how much IT is truly becoming the future, and the importance of being well informed in this field is suddenly being grasped. Consequently, many are seeking to educate themselves in blockchain development, and by so doing are positioning themselves for the career opportunities this innovation presents them now and in future.

CHAPTER SUMMARY

Blockchain has impacted the world in three specific ways:

- It has improved the speed and efficiency of financial transactions in most of the world.Moreover, it has brought more control to the public; personal control over one's finances has increased tremendously.

- Sensitization: The general public has become more aware of the advantages of possessing a skill in this space, and people are making moves to position themselves accordingly.

- It has led to intensified research by many corporations seeking to leverage the opportunities it presents.

CITATIONS

1. *How Blockchain Could Disrupt Banking*. (2021, February 11). CBINSIGHTS. Retrieved November 4 (what date is this book meant to be?) from www.cbinsights.com/research/blockchain-disrupting-banking/

2. The Leadership Network. (2020, January 22). *How Walmart Used Blockchain To Increase Supply Chain Transparency.* *https://theleadershipnetwork.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency*

CHAPTER 5:

WHO CREATED BLOCKCHAIN?

Can we give this title of creator to any one person?

As we have seen in the section briefly describing the history of blockchain, this technology's creation can be attributed to a collection of developments by not one person, but several individuals that contributed to its success at different points in time.

But the Bitcoin cryptocurrency is so far the first and—most successful—implementation of the blockchain system. The advent of Bitcoin has created an unprecedented awareness of blockchain technology's capacity to shape the future; so much so that blockchain and Bitcoin are considered by many to mean the same thing.

For this reason, the father of blockchain technology is unofficially accredited to Bitcoin's founder.

The identity of Satoshi Nakamoto, the founder of Bitcoin itself, has over the years remained a mystery. His last known communication was recorded as far back as 2011, two years after Bitcoin was brought into existence.

As Bitcoin has seen increasing success and enjoyed ever-increasing popularity, there have been attempts to bring the spotlight on certain individuals and point them out as the elusive Nakamoto. And while they received initial attention from the eager public, none has been proven beyond a reasonable doubt. We will examine three of the most near-successful proposals thus far, as evaluated by Investopedia. [1]

Dorian Nakamoto

This perhaps was the most high-profile attempt to reveal bitcoin’s founder. Newsweek in March 2014 identified Dorian Nakamoto as the currency's creator. Publication of the article caused a hullabaloo in the crypto and wider tech community, as this was the first time a mainstream publication had attempted to learn the identity of bitcoin’s creator.

Newsweek claimed several similarities between Satoshi Nakamoto and Dorian Nakamoto. For example, both supposedly held libertarian leanings and a Japanese connection. (Dorian, who graduated in physics from California Polytechnic and worked on classified defense projects, is Japanese-American). The article’s author also claimed Nakamoto said he was “no longer” involved with bitcoin and that he had “turned it over” to other people.

Dorian Nakamoto later denied the quote and claimed that he had misunderstood the question. He told the Associated Press, "I got nothing to do with it."

The magazine’s biggest mistake was to publish a photograph of Nakamoto’s home. A cursory image search could easily reveal its location. While many did not believe Dorian Nakamoto was bitcoin’s founder, the crypto community was aghast that his privacy had been violated.

Still, the media circus was not without profit for Dorian Nakamoto. An online campaign raised more than 100 bitcoins on his behalf. The fund was the bitcoin community's way of saying "thanks." In April 2014, Dorian Nakamoto appeared in a YouTube video along with fundraiser Andreas Antonopoulos to thank the bitcoin community for their support.

Craig Wright

For the most part, individuals suspected of being Satoshi Nakamoto have denied the claim or remained silent. That has not been the case with Craig Wright, an Australian scientist.

In December 2015, Wired Magazine wrote a profile on Wright, claiming it had "obtained the strongest evidence yet of Satoshi Nakamoto’s true identity.” The article reported on Wright's appearance via Skype at that year's Bitcoin Investors Conference in Las Vegas. When asked about his credentials, Wright claimed he was “a bit of everything.” He listed his degrees, including a master’s in statistics and two doctorates. He also said: "I've been involved with all of this for a long time...I try and keep my head down."

Wired's evidence consisted of references to a "cryptocurrency paper" on Wright's blog that appeared months before the bitcoin whitepaper began to circulate. In addition, there were leaked emails and correspondence with Wright’s lawyer that referenced a “P2P distributed ledger." Furthermore, leaked transcripts of meetings with attorneys and tax officials quoted him as saying: “I did my best to try and hide the fact that I’ve been running bitcoin since 2009. By the end of this, I think half the world is going to bloody know.”

Those claims were soon thrown into doubt. Wired followed up its report to note several inconsistencies in Wright's story. For example, the blog entries appeared to be backdated. Evidence also suggested that public encryption keys linked to Satoshi Nakamoto were also backdated. Even Ethereum co-founder Vitalik Buterin, who is otherwise reticent about politics in the cryptocurrency world, came out against Wright, publicly calling him a fraud.

But Wright remains unfazed by the criticism and has parlayed the media attention to carve out a prominent role within the crypto community. He led a contentious fork of Bitcoin Cash, forming Bitcoin SV. He is also chief science officer at nChain, a blockchain solutions business that serves enterprise customers.

Nick Szabo

Nick Szabo is a computer engineer and legal scholar. He is credited with pioneering the concept of smart contracts in a 1996 paper. In 2008, he conceptualized a decentralized currency he called Bit Gold, a precursor to bitcoin. He described Bit

Gold as "a protocol whereby unforgeable costly bits could be created online with minimal dependence on trusted third parties." This is similar to the bitcoin concept, whereby a series of bits created by a network of computers without a leader verify and validate transactions.

Author Dominic Frisby attempts to make the case that Nick Szabo is Satoshi Nakamoto in his book, Bitcoin: The Future of Money? Frisby consulted a stylometrics expert who concluded that Szabo's writing style was similar to known writings from Satoshi. Another clue is that both Szabo and Satoshi reference economist Carl Menger. In addition, Frisby learned Szabo had worked for DigiCash, an early attempt to bring cryptography to digital payments. In the author's eyes, this strongly suggested Nick Szabo is Satoshi Nakamoto.

While the identity of this mysterious innovator remains shrouded, it is agreed that deciding to remain anonymous was essentially a wise move to make. Also, the creation of blockchain technology can be attributed to not one person, but a number of individuals that contributed to its success at different points in times.

CHAPTER SUMMARY

Three men have been speculated to be Satoshi Nakamoto, the inventor of Bitcoin cryptocurrency:

- Dorian Makamoto
- Craig Wright
- Nick Szabo

CITATIONS

1. Sharma, R. (2020, August 21). *Three People Who Were Supposedly Bitcoin Founder Satoshi Nakamoto*. https://www.investopedia.com/tech/three-people-who-were-supposedly-bitcoin-founder-satoshi-nakamoto/

CHAPTER 6:

BENEFITS OF BLOCKCHAIN

Blockchain technology has gained a lot of popularity due to bitcoin transactions, but the technology has many uses beyond this application. It isn’t only needed to keep a record of the number of bitcoins exchanged but is an open ledger that isn’t owned by anyone. It is a technology that can be utilized for recording all types of sensitive information.

The global health chains, financial services, government, innovators, and industries are exploring new ways to utilize blockchain technology to transform and disrupt the business models abruptly.

By implementing blockchain technology, many businessmen have already reported the blockchain technology benefits such as greater transparency, improved traceability, enhanced security, reduced cost, verifiable speed, and reduced costs.

What Are the Benefits of Blockchain?

- **Greater Transparency**

Data and cash transactions are becoming easier through blockchain technology. All the participants of the networks share the same documentation instead of individual copies.

None of the participants change the documentation without changing the previous and subsequent documentation blocks. Therefore, blockchain technology is more accurate, consistent, and transparent when it is used in heavy processes.

- **Decentralization**

This is one of the greatest benefits of blockchain. A decentralized system isn’t controlled from a single source. It is an open-source system that cannot be traced by third parties—or even the government itself.

Whereas most systems (including our internet) are centralized, meaning that all the transactions done on the internet are traceable and can be seen by the government and third parties. this is completely the opposite when you use blockchain technology.

- **Reduced Costs for Businesses**

For most businesses in the world, reducing the cost is the main priority. With blockchain technology, you don’t need middlemen and outsiders to close deals. By using blockchain technology, you are not trusting the person but rather the data in the blocks.

Moreover, you won’t need to review the documentation over and again, as everyone will be provided with a single, unchangeable version of the documentation.

- **Voting Transparency**

Voting from a cell phone using a tested and safe interface can prevent fake and fraudulent votes.

In the current news, electronic voting under the eye of the government is being pursued, and one such example is the test of blockchain technology in electronic voting in Moscow.

Using blockchain technology will ultimately eradicate the chances of fraud in electronic voting. This is a huge achievement even though the electronic voting system is prevailing.

- **Data Ownership**

This is the key benefit of blockchain technology. Instead of being controlled from a single point, blockchain is widely spread. In blockchain technology, you own your data. No third party or government body can control its agenda and control your process. In short, blockchain is another name for a fair distribution system.

- **Enhanced Security**

In many ways, blockchain technology is much safer than other record-keeping systems. In blockchain technology, the transactions are based on trust and agreed upon even before they are recorded.

After that, when the transaction is done, it is linked to the previous transaction and hence, connected to the previous block. The information is shared on a large network of computers instead of a single server. This makes it extremely hard for hackers to get to your information.

It leaves no compromise on your data protection. Saving transactional data is very crucial for financial services and government bodies. Hence, blockchain technology can reduce electronic fraud and help people to do transactions safely over the internet.

- **Increased Efficiency and Speed**

When you stick to the traditional paper-based process, it becomes more time-consuming and prone to human errors. Moreover, it might also require third-party supervision. But that’s not the case with blockchain technology.

By streamlining your heavy processes through blockchain technology, the transactions can be carried out much more easily and efficiently. Since the documentation and single ledger are distributed with every individual, there will be much less clutter than usual.

Moreover, everyone would have the opportunity to access the same type of information. Hence, it would be easier for everyone to trust each other, and they won’t require any intermediaries.

- **Fraud Control**

A system in which data is stored in numerous networks of computers instead of just one is immune to the attack of hackers, as it becomes difficult to gain the overriding power required to make any changes to the stored information without being detected and challenged.

- **Quality Assurance**

A blockchain is fundamentally an open-source software for data transactions, resulting in its enhanced transparency. This transparency is consistently expressed in whatever form it is applied. Mainstream adoption of blockchain tech will bode well for any community, as it would set the standard for efficient and consistent data transactions.

- **Peer-To-Peer Global Transactions**

The integration of blockchain technology and cryptocurrency has enabled fast, secure and cheap transfer of money across the globe. Peer-to-peer transactions are cheaper and do not have taxes imposed on them. We can understand why more businesses now choose this option for international fund transfers.

- **Instant Settlements**

In blockchain technology, trust is important for carrying out money and data transactions, and as soon as your transaction is initiated, the settlements are instant. All you need is to trust the information that is being shared with you.

- **Health And Data Security**

The benefits of blockchain in health care are huge as well. For instance, digital medical records of patients backed up by blockchain technology could easily be retrieved by every medical facility regardless of the facility's location.

- **Driving Supply Chain Visibility**

The benefits of blockchain in supply chain management have amazed us in the past few years. The transformative technology offers more efficient and transparent mechanisms for managing inventory and recording all transactions.

CHAPTER SUMMARY

· Blockchain technology brings a lot of benefits for all that incorporate it into their systems, including (but not limited to):

- Greater Transparency
- Decentralization
- Reduced Costs for Businesses
- Voting Transparency
- Data Ownership
- Enhanced Security
- Increased Efficiency and Speed
- Fraud Control
- Quality Assurance
- Account Reconciliation
- Peer-To-Peer Global Transactions

- Instant Settlements
- Health Data Security
- Driving Supply Chain Visibility

CHAPTER 7:

BLOCKCHAIN USE-CASES

What does blockchain have to offer in the long term?

What industry stands to gain the most from this technology?

These are just a few of the questions on people's minds regarding this subject, and I can tell you with all certainty that we are yet to fully grasp how pivotal blockchain will be to solving a lot of real-world problems now and well into the future.

For this reason, a lot of people do not see blockchain technology offering anything beyond cryptocurrency. Yet, it has the potential to disrupt traditional technologies by reason of its ability to distribute power more evenly in many spheres—spanning finance, governance, supply chain management, and much more.

As we have already highlighted in "History Of Blockchain", there is almost no industrial sector that isn't looking to leverage the apparent advantages of the technology. In this guide, we will examine some of the practical applications that have been discovered for blockchain, detailing why they are needed now more than ever.

Transactions

As things stand, payment in almost every industry is made using some form of intermediary. This has two major downsides which include longer transaction time and higher fees. It even becomes worse when you're making international transactions, with the World Bank putting the average transaction fee at 7%.

As you already know, transactions on blockchain are done in a peer-to-peer manner which goes a long way in streamlining the process, completely taking out middlemen and resulting in shorter transaction processing time (as little as 5 seconds), while also shaving off a large percentage of the fees one would have been forced to pay by going through conventional channels. If we factor in the immutability and transparency of transactions, we might just about have the best solution for issues with global transactions.

Stellar, Ripple, and OMG Network are some of the cryptocurrencies that have been specifically designed to facilitate cheap, quick, and hitch-free global transactions.

Logistics and Supply Chain Management

Have you ever been to a store and wanted to cop limited-edition footwear—but you were suddenly concerned that it could be an imitation?

We all have been in such a scenario at one point or the other. This chapter will become endless if we go into details of all the challenges faced with supply chains (the process of getting a product from raw state to the final consumer). The processing of invoices, payments, logistics, and tax documents is time-consuming and could take weeks—months, even. Somewhere along the line, frauds, errors and other circumstances beyond anyone's control can lead to losses across the board.

McKinsey&Company give many use cases that prove the usefulness of blockchain tech in this industry.

“In most cases, today's supply chains operate at-scale without blockchain technology. Even so, the technology has excited the IT and supply-chain worlds. It has also inspired many articles and prompted established IT players and start-ups to initiate promising pilot projects, including:

“Walmart, which tested an application that traces pork in China and produce in the US, to authenticate transactions and the accuracy and efficiency of record keeping.

Maersk and IBM are working on cross-border, cross-party transactions that use blockchain technology to help improve process efficiency.

BHP is introducing a blockchain solution that replaces spreadsheets for tracking samples internally and externally from a range of providers.

Provenance, a UK start-up, just raised $800,000 to adapt blockchain technology to trace food. It previously piloted tracing tuna in the Southeast Asian supply chain.

“Yet to date, the authors are not aware of any at-scale applications to the supply chain, raising an essential question: Can blockchain technology add value to supply chains?

“Let's start with a reality check: As most practitioners know, many of today's supply chains have good data, which they are able to transfer across supply chain tiers at close to real time speed. To assess blockchain technology's value at stake for the supply chain world, we looked at three areas where it could add value:

“Replacing slow, manual processes. Although supply chains can currently handle large, complex data sets, many of their processes, especially those in the lower supply tiers, are slow and rely entirely on paper—such as is still common in the shipping industry.

“Strengthening traceability. Increasing regulatory and consumer demand for provenance information is already driving change. Moreover, improving traceability also adds value by mitigating the high costs of quality problems, such as recalls, reputational damage, or the loss of revenue from black-or grey-market products.

“Simplifying a complex supply base offers further value-creation opportunities (see sidebar, "A complex supply chain of unknown parties").

“Reducing supply-chain IT transaction costs. At this stage, this benefit is more theoretical than actual. Bitcoin pays people to validate each block or transaction, and requires people who propose a new block to include a fee in their proposal.

“Such a cost would likely be prohibitive in supply chains because their scale can be staggering. For example, in a 90-day period, a single auto manufacturer would typically issue approximately 10 billion call-offs just to its tier-one suppliers.

“Also, together all of those transactions would significantly raise demand for data storage, an essential component of blockchain's distributed-ledger approach.

“In addition, creating and maintaining numerous copies of data sets would be impractical in the supply-chain environment, especially in permissionless blockchains.” (McKinsey&Company,2017)

The transparency and immutability of data on blockchain ensure that everyone along the chain of supply is kept up-to-date with accurate information, thereby reducing conflict and delays. The fact that goods can also be tracked in real-time reduces the possibility of goods going missing.

FedEx, one of the most popular logistic companies in the world has partnered with BiTA and is utilizing a distributed ledger to track shipments. This has facilitated the speedy transfer of information and resolution of customer complaints; as it is very easy to point out where things went wrong.

Data Storage and Security

We live in an age where it is almost impossible to seclude yourself from the available information stream. In one way or another, the data you provide to access certain websites—or the data you save on cloud storage—are all kept on a centralized database. The direct implication is that your data can be lost by damage to centralized databases or prone to security breaches that could leave you exposed.

Storing data in distributed ledgers has improved the safety of cloud storage. This data can also be accessed across several nodes of the network, which means any data attack won't be fatal and there will be no way to modify or steal data stored on a blockchain.

NuCypher is one of the foremost security and encryption platforms for distributed systems, which employ and combine the features of blockchain, big data, cloud, and the Internet of Things (IoT).

Contracts

Contracts generally come into play as a result of a lack of trust between the parties involved. We go through a lengthy process involving several parties and loads of paperwork; this is without even factoring in what we get to pay the lawyers involved. The entire process seems fine and worth it until you realize how much easier this could be by making the contracts SMART.

The Ethereum blockchain, one of the most popular around, was specifically built for this purpose. A smart contract is simply lines of code stored on a blockchain that is designed in such a way to execute a command as soon as certain conditions are met. The immutable and open nature of blockchain then ensures that anyone can view the terms of the contract without being able to edit it.

TradeIX currently offers distributed technology solutions that are directed towards alternative funders, banks, and value-added providers. They enable financial institutions to offer their clients a top-notch user experience while reducing costs and risks.

Healthcare

The manner in which healthcare records are stored is such that there have been innumerable cases of data breaches over the years, not to mention the poor state of interhospital communication. In cases of emergencies, the newly established hospital is often forced to create new records, thereby wasting time and valuable resources.

With the introduction of blockchain, we can have a decentralized log of all patient data, accessible by all hospitals. Patients need not worry about data privacy, as their stored data will be untraceable to them unless they—or the hospital—decide to part with it.

Medicalchain blockchain protects patients' data from external sources while establishing a single point of truth for all data.

Guardtime is mainly concerned with the cybersecurity aspect of healthcare. They have implemented blockchain technology into Estonia and the UAE's healthcare systems.

Real Estate

The real estate industry is in a serious mess that many realtors often fail to admit. It isn't just enough to have money to get a property; the tedious process along with cases of seller fraud makes it an industry only for the experienced heads.

You can as well digitize your real estate assets and store them in a distributed ledger, making them immutable. This step makes it impossible for anyone to sell a property they do not own. Furthermore, you can make use of smart contracts to simplify and automate most of the paperwork and legalities.

PropertyClub and Propy are two different organizations that enable users to carry out the exchange of real estate assets digitally and securely. They also facilitate tokenization of real estate assets in order to ensure transparent transactions.

Government and Voting

Most of the processes in government today still rely on outdated and ineffective methods. It is a known fact that internal data breaches render the government very vulnerable. The centralized nature of things like voting also gives room to corruption within the government, thereby fostering distrust between the government and its people.

The use of smart contracts in government will ensure a lot of labor-intensive tasks become automated, which goes a long way in reducing the cost of operation. The decentralized and transparent nature of blockchain will build trust between the people and those in power. Introducing blockchain-based voting systems will also obliterate forced voting, miscounts, and machine hacks while ensuring the complete anonymity of the voter.

The UAE will be one of the very first countries to implement a blockchain policy. They aim to capitalize on the technology to transform as much as 50% of government operations by the time 2021 runs out.

In all this, one thing that seems certain is the fact that blockchain technology does have a future loaded with numerous possibilities in several industries. While many skeptics do not see the need for blockchain in several industries, many experts believe otherwise.

CHAPTER SUMMARY

The following use-cases show just how much practical application has been achieved with blockchain technology.

- Stellar, Ripple, and OMG Network are some of the cryptocurrencies that have been specifically designed to facilitate cheap, quick, and hitch-free global transactions.

    - Walmart, IBM and other companies have recorded successful implementation of blockchain tech for their tracking processes.

    - In the case of data storage andsecurity, NuCypher is one of the foremost security and encryption platforms for distributed systems, which employ and combine the features of blockchain, big data, cloud, and the Internet of Things (IoT).

· The Ethereum blockchain has succeeded in making contracts SMART (able to run automatically, without intermediaries).

· In Medicine, Medicalchain blockchain leverages blockchain to protect patients' data from external sources while establishing a single point of truth for all data.

· Real Estate: PropertyClub and Propy are two different organizations that enable users to carry out the exchange of real estate assets digitally and securely. They also facilitate tokenization of real estate assets in order to ensure transparent transactions.

- Government: The UAE will be one of the very first countries to implement a blockchain policy. They aim to capitalize on the technology to transform as much as 50% of government operations by the time 2021 runs out.

CITATIONS

McKinsey&Company. (2017, September 12). *Blockchain technology for supply chains—A must or a maybe?* https://www.mckinsey.com/business-functions/operations/our-insights/blockchain-technology-for-supply-chainsa-must-or-a-maybe

PART II:

BLOCKCHAIN ECOSYSTEM

CHAPTER 8:

BLOCKCHAIN COMPONENTS

There are many implementations of the blockchain technology that have indirectly worked together to create blockchain universe—or rather, a universe with many worlds. We will now look at some of the core parts of this massively growing system.

BLOCKCHAIN EXCHANGES

Every Blockchain project has a robust ecosystem working under it, based on a decentralized exchange. These are developed by the Blockchain team or the community of other developers. A typical exchange is designed to find the cheapest rates of exchange between any two cryptocurrencies, making it more affordable to trade tokens/cryptocurrencies. Exchanges are used for trading and can be integrated with hardware wallets, or users can create their wallets on the exchange websites.

BLOCKCHAIN MINERS

For a blockchain to function and maintain its integrity, it needs a large network of independent nodes from around the world to maintain it continuously. In a private blockchain, a central organization has authority over every node on the network. On the other hand, in the case of a public blockchain, anyone can set up their computer to act as a node. The owners of these computers are called miners. Since the integrity of the blockchain is directly related to the number of independent mining nodes in the network, there also exists an incentive model for mining. Different blockchains utilize different mining systems. However, most of them contain some form of an incentive system or a consensus algorithm in the blockchain network. Let us examine some of them.

CONSENSUS ALGORITHM

What is a Consensus Algorithm?

A consensus algorithm is simply a mechanism used to establish agreement on a single data value across distributed systems. It is a process through which all parties on the blockchain network arrive at a common agreement on the current data state of the ledger. Its importance to a blockchain network cannot be overemphasized as it is the key component that maintains the integrity and security of the distributed ledger.

For a consensus algorithm to be considered useful, it must fulfill every one of the following:

Unification of Agreement: Unlike centralized systems where it is necessary to trust the authority in charge, a decentralized setting has no such requirement as users can operate without even having an iota of trust for anyone. The inherent consensus algorithm embedded in the distributed ledger ensures that the data involved in the process is accurate and true.

Prevention of Double Spending: The consensus mechanism ensures that only verified transactions are input in the public ledger. This obliterates the scenario where an individual can use the same currency for two different transactions.

Fault Tolerance: This simply refers to the ability of a system to keep operating seamlessly and without interruption when there is a failure of one or more of its components. The consensus algorithm in this case ensures that there are backup nodes to take the place of failed components, which in turn prevents the network from experiencing any downtime.

Popular Blockchain Consensus Models

Proof of Work (PoW)

This is the process through which a cryptographic hash is produced. It was first introduced by Cynthia Dwork and Moni Naor in 1993 but was made popular when it was later utilized by Satoshi Nakamoto for Bitcoin in 2008.

In this algorithm, miners are required to solve complex mathematical problems using different mining methods with the common factor being very high computation power. The reward for successfully solving this problem is a new block integrated into the chain, and some coins to the miner.

The PoW is a resource-intensive protocol that feasts on computational power and electricity to solve the cryptographic puzzles it was intended to. Apart from Bitcoin, the PoW is currently being used in several other cryptocurrencies which include Montero, ZCash, and Litecoin.

Proof of Stake (PoS)

This consensus algorithm was created as an alternative to PoW in 2011. Though meant to achieve the same objective, there are some fundamental differences.

In this algorithm model, the block producers do not concern themselves with mining, and the term "validator" more aptly describes what they do.

For an individual to become a validator, he must invest/stake some amount of money; usually the localized digital currency of the blockchain in question. The reward system in this algorithm is based mainly on the amount you have staked (the more coins you have locked, the higher your reward). However, if you attempt to game the system by proposing invalid transactions, there's a possibility you could lose all your stake.

Proof of Burn (PoB)

"Burning" in blockchain lingo, simply means sending a valuable coin to an inaccessible account.

In the PoB algorithm, validators earn the privilege to mine based on a random selection process which is greatly influenced by how much coin one is willing to ditch.

Many experts believe that the PoB algorithm is a great alternative to PoW considering how environmentally friendly it is comparatively. However, it is a general belief that it still needlessly wastes resources.

Proof of Elapsed Time (PoET)

This PoET was developed by Intel to obliterate the mathematical puzzles associated with the PoW model. The algorithm is mostly used in permissions blockchain ledgers with the IBM's Hyperledger Sawtooth being one of its main applications.

The PoET operates using a randomized timer system for network participants. Each participant is given a random timer object and the participant whose timer expires first earns the privilege to produce a new block.

Proof of Capacity (PoC)

In the Proof of Capacity mechanism, intending validators are expected to invest their hard drive space for the production of blocks. Just like in almost all the other mechanisms, the system is resource biased, with people investing more hard disk space being prioritized within the ecosystem.

These are just a few of the most popular algorithms in existence. There are others like Proof of Authority, Proof of Weight, Proof of Importance, Proof of Activity, Proof of Identity, and Byzantine Fault Tolerance. It is therefore an important factor to critically consider what is best suited to a project before choosing a consensus algorithm.

CHAPTER SUMMARY

There are many implementations of the blockchain technology that have indirectly worked together to create blockchain universe—or rather, a universe with many worlds and some of the core parts of this massively growing system include:

· Blockchain exchanges, where tokens and cryptocurrencies are mostly traded.

· Miners, who are the lifeblood of the blockchain network. Their activity ensures its continuity.

· Consensus algorithms, a mechanism used to establish agreement on a single data value across distributed systems.

- Popular blockchain consensus models include:
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Proof of Burn (PoB)
  - Proof of Elapsed Time (PoET)
  - Proof of Capacity (PoC)

CHAPTER 9:

TYPES OF BLOCKCHAIN TECHNOLOGY

Everyone has begun witnessing the potential of blockchain with the increasing demand for this technology. In its initial days, blockchain brought a disruption to the financial industry, but now its uses have been accepted across various industries.

Since organizations have started to explore the capability of this technology by building blockchain applications, the demand for blockchain platforms has risen exponentially. So now, we are coming to an essential point—which is understanding the different blockchain technologies available in the market.

BITCOIN

The starting point of blockchain was Bitcoin. Satoshi Nakamoto introduced Bitcoin in his white paper of 2008, and Bitcoin was the first cryptocurrency to come into the market. In 2008, he created Bitcoin, and in 2009 he made it public.

Bitcoin represented the introduction of cryptocurrencies and their potential in this world. The Blockchain network uses transactions to create other transactions, and Bitcoin uses those exact transaction mechanisms. We call them 'unspent transaction outputs'. The main principle behind a Bitcoin transaction is that the transactions themselves are interlinked. Then, there are scripts which are the validation processes for Bitcoin transactions. They validate whether one person has five Bitcoins to transfer to friend A and whether friend A has a valid address (which is a valid account inside the Bitcoin network where you want to make the transaction). Scripts also check whether these transactions are being recorded on different networks or a private peer-to-peer network. Scripts verify and validate Bitcoin transactions. Then there is metadata. Metadata is the data associated with the transactions. Currently, on the Bitcoin network, you can send up to 1MB of data with your transaction.

Metadata carries details about the transaction and any additional comments you want to add to the Bitcoin transaction. Metadata can be used in two ways, as a storage unit as well as a database unit where you are storing some data. Because the transaction happens on the Bitcoin network, it is a permanent transaction that cannot be changed or tampered with, and you can then use the data within your applications or projects. Moreover, there is a consensus algorithm known as the Proof-of-Work algorithm, which in conjunction with the timestamp of the transaction, validates the block.

Proof-of-Work means any transaction that happens on the Blockchain network that has some associated puzzle to be solved for that transaction to be successful. By puzzle, we mean the ‘nonce,’ which is a random number that the miners are trying to work out.

ETHEREUM

Ethereum is a blockchain that is based on Bitcoin but has certain functionalities that make it much stronger in the market. Ethereum is the brainchild of Vitalik Buterin. He came up with a process whereby *Turing-complete virtual machines* are created, called the *Ethereum Virtual Machine*.

Ethereum is a mathematical project in which systems are created with the primary function of building smart contracts. Smart contracts are currently used in various ways behind major systems. To get you started with smart contracts, think of them as traditional paper-based contracts, such as rental agreements, but online instead. Within the smart contracts, you can mention certain rules which all the parties connected to it will need to follow.

When Ethereum started, it was created in a language called Solidity. Solidity is a combination of C++ and JavaScript; it's not too difficult to learn. So, the main challenge faced by Ethereum is scalability. Ethereum is currently trying to solve that problem, and they have come up with a new consensus protocol called Proof-of-Stake.

Up until now, we have only discussed the Proof-of-Work algorithm where the miners are trying to guess the nonce. When they even come close to the random number, the transactions are confirmed.

Proof-of-Stake takes a different trail. With Proof-of-Stake, you need to have some stake (cryptocurrency) on the Blockchain itself, i.e., stakeholders. Imagine that a Blockchain has 100 coins, where person A has a stake of 80 coins, and person B has a stake of 20 coins. Now, whenever a transaction happens, there is a specific fee applicable to that transaction. There is a certain fee associated with the transaction which is being awarded to the miners, apart from the block mining rewards.

In contrast, while using Proof-of-Stake, whenever a transaction happens, person A will take 80% of the fees, and person B will receive 20% of the fees because A has 80% of the coins on the Blockchain and B has only 20% of the coins. The percentage of your stake determines the percentage of fees you will receive. While Ethereum is still using Proof-of-Work, they are working hard on developing Proof-of-Stake for use.

HYPERLEDGER

Hyperledger started as an open-source collaborative effort to create a platform for developing your blockchain solution. One of the essential characteristics of Hyperledger is that it does not support any cryptocurrency, unlike Bitcoin and Ethereum which have their native cryptocurrencies. The

Linux Foundation established this platform in 2015.

Currently, Hyperledger is provided for by almost 100+ members, and this includes technological giants like IBM, Intel, Samsung, J. P. Morgan, etc.

It is a Blockchain platform within which you can define your own rules, permissions, and efforts to host a blockchain. It acts as the operating system of marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities. It has the potential to vastly decrease the expenses and complications in getting things done in the real world. For example, if you want to host your public chain, there is a very complicated procedure for doing so. But with Hyperledger, the software proves that it is effortless to host your public blockchain so that you can create smart contracts.

BLOCKCHAIN DEVELOPERS

Blockchain technology is built by the potential developers working on it. A strong team of developers can establish an incredible blockchain project.

Blockchain developers build new blockchains with different levels of functionalities and consensus algorithms. App developers work with decentralized applications that can run on Blockchains, thus providing a similar functionality like Google Play Store over blockchain Technology. The development of smart contracts over a Blockchain has opened the possibility for developers to create extensive applications and use cases for industries.

BLOCKCHAIN APPLICATIONS

Apart from exchanges, platforms, and users, another vital aspect of the blockchain ecosystem is the development of applications that industries, developers, and communities build to serve a specific purpose. There are various examples of applications being built upon the blockchain, and we will examine some of them.

1. CryptPad:

What is CryptPad?

CryptPad is a private-by-design alternative to popular office tools and cloud services. All the content stored on CryptPad is encrypted before being sent, which means nobody can access your data unless you give them the keys.

CryptPad is a suite of zero knowledge, realtime collaborative editors and applications. Encryption carried out in your web browser protects the data from the server, the cloud, and the NSA. The secret encryption key is stored in the URL fragment identifier which is never sent to the server but is available to javascript so by sharing the URL, you give authorization to others who want to participate.

CryptPad uses a variant of the Operational transformation algorithm which is able to find distributed consensus using a Nakamoto Blockchain, a construct popularized by Bitcoin. This way the algorithm can avoid the need for a central server to resolve Operational Transform Edit Conflicts and without the need for resolving conflicts, the server can be kept unaware of the content which is being edited on the pad.

Cryptpad offers collaboration on text and WYSIWYG documents, as well as a basic polling application where users see results in real time.

2. Humaniq:

Humaniq is a fintech startup connecting un- banked people with the global economy. “Humaniq aims to increase financial inclusion worldwide by providing new financial services to the unbanked based on Blockchain technology and biometric identification systems. With this new mobile digital economy, we will help people who are excluded from the financial system break free from poverty and improve their lives, and emerging economies shift into the cryptoeconomy."

3. Augur: Augur is a peer-to-peer oracle and prediction market place or Filament, which is Building IoT (Internet of Things) applications over the blockchain.

In a review by Ryan Berckmans of Predictions

Global, “Augur is a substitute for betting platforms that charge high fees, ban winners, delay withdrawals, freeze accounts, aren't globally accessible, lack privacy, and don't let you sell your bet mid-game.”

CHAPTER SUMMARY

- There are a number of blockchain systems that have gained prominence within the ecosystem:
    - Cryptocurrency blockchain. Bitcoin represented the introduction of cryptocurrencies and their potential in this world. The Blockchain network uses transactions to create other transactions, and Bitcoin uses those exact transaction mechanisms.

    - Ethereum is a blockchain that is based on Bitcoin but has certain functionalities that make it much stronger in the market. Ethereum is a mathematical project in which systems are created with the primary function of building smart contracts.

- Hyperledger

There are various examples of applications being built upon the blockchain, some of which are:

1. CryptPad, a private-by-design alternative to popular office tools and cloud services.
2. Augur, a peer-to-peer oracle and prediction market place or Filament, which is Building IoT

(Internet of Things) applications over the blockchain.

3. Augur, a peer-to-peer oracle and prediction market place or Filament, which is Building IoT (Internet of Things) applications over the blockchain.

CITATIONS

1. *Ansuz*. (2016, July 12). *CryptPad.* AlternativeTo. https://alternativeto.net/software/cryptpad/about/#:~:text=CryptPad%20is%20a%20private-by-design%20alternative%20to%20popular%20office,of%20zero%20knowledge%2C%20realtime%20collaborative%20editors%20and%20applications.

2. *About Humaniq*. Retrieved Nov 3, 2020, from https://humaniq.com/about#:~:text=Humaniq%20aims%20to%20increase%20financial%20inclusion%20worldwide%20by,based%20on%20Blockchain%20technology%20and%20biometric%20identification%20systems
.

CHAPTER 10:

PUBLIC AND PRIVATE BLOCKCHAINS

PUBLIC BLOCKCHAIN

A public blockchain, also known as a permission less blockchain, is open to all, and everyone can read as well as write over the data. In a public blockchain, you don’t need any authorization as you have open access to all the data. Moreover, if the blockchain is public, the rules are very complicated, along with a complex consensus algorithm for better security.

We will discuss complex consensus algorithms in detail, along with Proof-of-Work and Proof Of-Stake. Miners use these algorithms to confirm transactions over the blockchain.

A public blockchain has more complex consensus algorithms as compared to a private blockchain because, in a private blockchain, the permission is limited to a group of people who are accessing the network. So in a private blockchain, you don't need miners to solve a complex problem and spend precious time confirming mammoth volumes of data.

In the case of a complex consensus algorithm, they are computationally more expensive to mine into a block. No one owns a public blockchain; hence it has no central authority or single person over it. Even Satoshi, who started the white paper for bitcoin, transferred everything to the public in 2009. So all public blockchains are open, which means no one owns them, and you can read and write data over them. The Bitcoin blockchain and Ethereum Blockchain are the best examples of public blockchains.

PRIVATE BLOCKCHAIN

A Private Blockchain, as the name suggests, is for personal use. It can be used with your existing applications to make them even more secure. Such networks allow you to provide significant permissions—like authorizing the nodes connecting to the network. Nodes are nothing but different computers connected inside the peer-to-peer network running the blockchain codes.

In a private blockchain, you can provide permissions as to who can read the data and who can transfer the data. You can even offer authorization in a way that only person A has the permission to transfer money, and person B can only view this data.

Private blockchains have less security as compared to a public blockchain because, in a private blockchain, we make it easily accessible to a certain trusted group of people and not millions. Also, if you are using a private blockchain (like Hyperledger or Corda), then you can have the same kind of security as a public Blockchain or bitcoin, and one authorized node can be the arbitrator for any dispute.

Now you know that the private blockchain is for those who want to have more control over the blockchain; who want to be the authority governing the blockchain. A few good examples of private blockchains are RecordsKeeper Blockchain, Hyperledger, Corda, Quorum, etc.

CHAPTER SUMMARY

There are two blockchain categories:

1. A public blockchain, also known as a permission-less blockchain, is open to all, and everyone can read as well as write over the data.

2. A Private Blockchain, as the name suggests, is for personal use. It can be used with your existing applications to make them even more secure.

PART III:

INTRODUCING SMART CONTRACTS

CHAPTER 11:

SMART CONTRACTS

The name "Smart Contract" is increasingly mentioned when blockchain or general advancement in tech is discussed. While many are familiar with the term, very few people truly understand what it is, and what it does.

What exactly is a smart contract?

A Smart Contract is an automated program stored on a blockchain, designed to execute a certain task once the specified conditions for it are met.

First, let us gain a general knowledge of what a traditional contract is, thereby laying the groundwork for a thorough understanding of smart contracts.

In very simple terms, a contract can be defined as a binding agreement between two or more parties and is usually enforceable by law. Contracts have become part and parcel of everyday dealings in all spheres of life; therefore, a good understanding of the rules of every contract is required in order not to get shortchanged. A contract generally needs an offer, consideration, acceptance, and mutual intent to be bound before it can be considered valid.

Introducing Smart Contracts

Nick Szabo was the first to describe what a smart contract should look like in the year 1994. In illustrating the concept, he employed the vending machine.

An individual inserts money into a vending machine, selects his desired item, and provided the amount is correct, the vending machine will deliver the goods requested.

This interaction requires no trust between the two parties and is the same principle guiding smart contracts. The technical infrastructure (program) already in place guarantees that the contract will be fulfilled. In other words, smart contracts make a breach of the contract impossible.

When the conditions set out in a smart contract have been met, the terms stated before that are automatically enforced on the blockchain. If we then consider the fact that transactions so completed are immutable, it becomes conclusive that it is safe and easy to do business with anyone, whether you trust the person or not.

HOW A SMART CONTRACT WORKS

To explain this in a way that can be easily understood, we will highlight the concept of crowdfunding platforms.

Crowdfunding platforms involve projects that many supporters make contributions to. A project is broadcasted along with its financial requirements, and different people fund it by making contributions in volumes of their choosing until the target for the project is met.

While contributions are being made, the platform holds onto the money until the set target is reached before releasing it all to the project team; then the project kicks off.

A smart contract works similarly, except that the whole process is programmed and stored in a blockchain network.

So, if a smart contract is created for a fundraising project, the supporters can simply send their contributions to the smart contract, which by design would hold all funds received. The conditions here are that:

1. If the target amount is reached, the smart contract automatically releases the funds to the creator(s) of the project.

2. On the other hand, if the target is not reached (very likely at the end of a specified time frame), the smart contract will automatically reverse the money contributed to its senders.

Thus, smart contracts are created and executed: a condition—or a set of conditions—is agreed upon, an automated program is created and stored on a blockchain network to 'oversee' the process of the contract, which is finally engaged by the involved parties.

CHAPTER SUMMARY

- A Smart Contract is an automated program stored on a blockchain, designed to execute a certain task once the specified conditions for it are met.

- When the conditions set out in a smart contract have been met, the terms stated before that are automatically enforced on the blockchain.

- Smart contracts thus created and executed: a condition—or a set of conditions—is agreed upon, an automated program is created and stored on a blockchain network to ‘oversee’ the process of the contract, which is finally engaged by the involved parties.

CHAPTER 12:

HOW DO SMART CONTRACTS BENEFIT US TODAY?

You might already be thinking, "why do we need smart contracts when traditional contracts are working out just fine?"

Well, the truth is that we are naturally inclined to believe an existing model to be the best until we are presented with something different. Here are some advantages worth considering in regards to this new method of contracts:

1. SPEED AND EFFICIENCY

To truly understand the downsides to a traditional contract, consider yourself intending to get a loan from a bank for which you are required to provide collateral. Vetting the property to be used as collateral, approving funds, and deposit into your account is a multi-step process that will involve multiple parties along with lots of paperwork that you and all intermediaries would have to fill. All this takes considerable time while causing both parties to incur avoidable costs simply because of a lack of trust between transacting parties.

This prolonged, overblown process was indicative of the need for a more efficient system of sealing deals—which has now come in form of Smart Contracts.

With smart contracts, once the value of the collateral is validated, the loan is approved by the contract and immediately effected, with no need for intermediaries. Only the parties directly involved with the engagement are required. This way, not only time, but extra money, is saved.

2. TRUST

In the funding illustration we used earlier, all parties involved would have to trust the platform (third-party) to execute the contract satisfactorily: the project team would expect to be given their money, and the supporters would likewise expect their contributions to meet their intended recipient—or else to be returned to them if the goal is not reached.

Not so with smart contracts.

Why?
Because by being implemented on the blockchain, smart contracts inherit the DLS (Distributed Ledger System) and the immutability (non-reversible) properties of the blockchain. Immutability means that once a smart contract is created, it cannot be altered or reversed. The distributed nature also makes it so that all the parties involved (in this case, the project creator and the supporters) validate the output of the contract. So, no one person can succeed in trying to force the funds to be released; all the other participants in the network will spot and discard the attempt as invalid.

For these reasons, smart contracts command absolute confidence and trust in their ability to execute transactions smoothly.

3. SIMPLICITY AND CLEAR COMMUNICATION

Typical traditional contracts are oftentimes quite lengthy, burdensome, and full of complicated language that needs lawyers to create and decipher. Smart contracts take away this pain just by being programs.

Because they are automated programs, smart contracts require that every term and condition included in them are explicit in detail, as any kind of omission or vagueness will result in a transactional error (something to be greatly wary of, when you recall that smart contracts are permanent once written).

This makes for contracts whose terms are clear, easily understood, and agreed on by all—a tremendous relief to the parties involved.

4. TRANSPARENCY

In addition to being simple and easily understood, the terms of a smart contract are also visible and accessible to all the parties involved in the contract, thereby facilitating complete transparency of the transaction.

5. SECURITY

Automated contracts employ the highest encryption format available—the same standard that cryptocurrencies use today. The implication of this is that smart contracts are among the most secure transactions that can take place online.

6. STORAGE/BACKUP

The decentralized and permanent storage of details makes smart contracts reliable in terms of backup and storage, as such details can be easily retrieved whenever needed. This is naturally a preferable option to reliance on paper records that can be compromised by a variety of circumstantial factors—or even digital records that are stored in one or a few locations when contrasted with the tens, hundreds, or even thousands of storage locations that come naturally with smart contracts.

7. RELIEF

From the need to hire lawyers (and settle them) to the accumulation of heaps of paperwork, while contracts are a necessity, so also are they quite burdensome in their merciless demand for time, money, materials, and mental resources. Making contracts smart automatically ushers an all-round respite from such demanding tasks.

LIMITATIONS OF SMART CONTRACTS

With all that has been mentioned on this subject, it would seem that smart contracts are the way to go now.

However, this innovation is yet to witness full integration in its applicable fields. Here are four major factors that presently hold it back from taking over its traditional elder. Some of these challenges are present in the very factors that are meant to give smart contracts the upper hand.

1. LOOPHOLES

The digitalized nature of smart contracts means that they are vulnerable to loopholes and oversights during their creation. Such omissions are not a new thing; revisions and crosschecks would normally fix them. So, this would normally not be a serious issue—until you consider the fact that smart contracts, once written, are permanent.

2. IMMUTABILITY

The inability of smart contracts to be changed presents a problem: this immutability extends to any errors that may happen in the coding process. Short of creating a whole new contract, it is near-impossible to fix such errors should they occur.

3. THIRD PARTIES

Even as smart contracts try to eliminate the need for third parties, that is not (yet) entirely possible. Lawyers for instance may no longer be needed to prepare the contracts, but programmers will certainly need them to be able to fully understand the terms and encode them into the automated structure.

Besides, smart contracts are themselves intermediaries between the parties involved in the execution of their agreement, making them third parties in a way—only they're not humans.

4. VAGUE TERMS

Because smart contracts demand simplicity and explicitly laid out terms, some of the more complicated and vague terms present in contracts pose a challenge for smart contracts, as they may not be able to include them. This makes smart contracts most suitable for agreements featuring the simplest of terms and conditions in their execution.

As is common with the most disruptive of inventions, smart contracts still have a few grey areas that have the majority initially sticking with the methods that have worked quite fine for them in the past.

These hurdles are not insurmountable, however. The benefits they proffer make them worth the continued investment and effort made at improving them. It is very safe to conclude that smart contracts will find ways around whatever challenges they are currently encountered with—and ultimately take over to become the new traditional means of sealing deals.

WHY DO SMART CONTRACTS NEED BLOCKCHAIN?

As earlier highlighted, the concept of smart contracts existed long before the advent of blockchain. However, not until blockchain came to the fore were the ideas able to be implemented.

This is without a doubt, a case of one innovation waiting on the arrival of another for the both of them to reach their full potential.

In an ideal situation, the concept of a smart contract described by Nick Szabo required a completely decentralized system which was non-existent at the time. However, with the advent of blockchain technology, smart contracts were able to leverage it to verify, validate, capture and enforce agreed-upon terms between multiple parties without the influence of a third party.

Blockchain can be termed the ideal operating environment for smart contracts, as all the stored data is immutable and safe.

WHAT INDUSTRIES STAND TO BENEFIT THE MOST FROM SMART CONTRACTS?

This technology has found compatibility with the following industries:

- Banking and Finance

- Real Estate
- Insurance
- Healthcare

Clear and understandable rules, algorithms, and quantifiable engagements are the substance forming their structure, making them the perfect fit for smart contracts.

Industries such as food and hospitality, on the other hand, are less compatible with the technology due to the qualitative nature of their services.

BLOCKCHAINS THAT SUPPORT SMART CONTRACTS

There are more blockchains than we can count in existence today. However, each one has a major purpose which would have been highlighted in its whitepaper.

We will be dwelling on a few of those with smart contract capabilities. These include;

Ethereum

Ethereum, unarguably one of the most popular applications of blockchain, was created in 2014 by Vitalik Buterin and was designed specifically for building smart contracts. It has done exactly that, as it remains the most popular platform for creating smart contracts to date. Its community—without doubt the most active blockchain community within this sphere—is made up of app programmers, core protocol developers, mining organizations, and many others, including ordinary users.

Ethereum makes use of the Solidity programming language which is simple enough that anyone with a reasonable understanding of coding can begin to write smart contracts for the Ethereum Virtual Machine (the central piece that interprets all commands). There are hundreds of applications like MakerDAO and Compound which already leverage the smart contract capabilities of Ethereum to facilitate lending while allowing users to earn interest.

In a simple example of how the Ethereum smart contract can be utilized, Mike sends 5 Ether (the native token of the Ethereum blockchain) to Paul. He can choose to disperse the coin release over a specific period or even set out conditions that need to be met before the coin is released.

NEO

NEO, also a very popular blockchain project in most of Asia, facilitates the execution of trustless smart contracts. It has been nicknamed ‘China’s Ethereum Killer' mostly due to its similarity to Ethereum and where it first found roots.

NEO, as opposed to Ethereum, enables developers to write smart contracts in languages they already understand, making it so much easier to execute. NEO operates a dual token ecosystem, with the main token being NEO and the other, GAS (which is automatically mined when users hold NEO in a specific wallet).

The most distinct advantage of NEO over Ethereum is the simplicity with which any programmer can build smart contracts.

Hyperledger Fabric

Hyperledger is an open-source blockchain framework that is hosted by the Linux foundation. It facilitates the creation of enterprise-grade, distributed ledger frameworks for the execution of smart contracts called chaincode. Smart contracts on Hyperledger are written in the Go programming language.

The modular approach which is employed in building blockchains by Hyperledger along with ample scalability helps companies to develop what suits them best. This has been a major selling point for them and has attracted reputable companies like Intel, Samsung, and J.P.Morgan.

NEM

NEM was launched in March 2015. Since then, it has become a popular choice amongst blockchain developers, as codes are written using Java, a familiar programming language to many developers around the world. This implies that programmers do not have to learn blockchain platform-specific languages like Go and Solidity.

NEM is believed to be one of the most secure smart contract platforms available for use. The NEM blockchain is highly scalable while being able to process hundreds of transactions per second as opposed to the fifteen per second achievable on Ethereum.

WAVES

This is an open-source platform launched in June 2016 and aimed to address existing obstacles standing in the way of widespread blockchain adoption, mainly speed and scalability.

Apart from being an ideal platform for building smart contracts, WAVES is an excellent platform for conducting Initial Coin Offerings (ICO). Very little technical knowledge is needed to create your token on the platform. For all the simplicity it offers, the major downside to WAVES is its relatively small user base, which makes it pretty difficult to get help within the community.

There are loads of other smart contract-rendering blockchains apart from the five listed above, each with its specific advantage. Your duty as a smart contract programmer will simply be to find the one that best suits your project.

CHAPTER SUMMARY

Smart contracts have been found to be quite beneficial in no few ways:

- Speed and efficiency in transactions.
- Trust is no longer an issue, as the conditions, once determined, must be adhered to.
- Simplicity and clear communication is the requirement for setting conditions for smart contracts, making them easier to understand.
- Transparency is enforced by immutability.
- Security in smart contracts are high-end, as they inherit the security protocols of the blockchain network.

- The decentralized and permanent storage of details makes smart contracts reliable in terms of backup and storage.

  - From the need to hire lawyers to the accumulation of heaps of paperwork, making contracts smart automatically ushers an all-round respite from such demanding tasks.

Smart contracts also have some limitations:

- The digitalized nature of smart contracts means that they are vulnerable to loopholes and oversights during their creation.

- The inability of smart contracts to be changed means that if any error occurs during creation, it cannot be changed.

· Smart contracts are really only most suitable for agreements featuring the simplest of terms and conditions in their execution.

· The blockchain system is the ideal operating environment for smart contracts, as all the stored data is immutable and safe.

· Smart contracts have found compatibility with the following industries:

- Banking and Finance
- Real Estate
- Insurance
- Healthcare

- There are more blockchains than we can count in existence today, but not all of them support smart contracts. Here are some that do:

  - Ethereum
  - NEO

PART III:

CRYPTOGRAPHY AND CRYPTOCURRENCY

CHAPTER 13:

INTRODUCING CRYPTOGRAPHY

Cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process.

Cryptography is also made up of two ancient greek terms, Kryptos and Graphein, the former term meaning “hidden” and latter; “to write”.

There are several terms related to cryptography, which are stated as follows:

Encryption: It is a process of converting a plaintext (normal text) into a ciphertext (random sequence of bits).

Decryption: The inverse process of encryption, conversion of ciphertext to plaintext.

Cipher: The mathematical function, i.e. a cryptographic algorithm which is used to convert plaintext to ciphertext.

Key: A small amount of information is required to induce the output of the cryptographic algorithm.

TYPES OF CRYPTOGRAPHY

Symmetric-Key Cryptography: In this encryption method, we take a single key into the application. This common key is used for both the encryption as well as the decryption process. Using a common single key creates the problem of securely transferring the key between the sender and the receiver. It is also called Secret-Key Cryptography.

Asymmetric-Key Cryptography: This encryption method uses a pair of keys: an encryption key and a decryption key named public key and private key respectively. The key pair generated by this algorithm consists of a private key and a unique public key that is generated using the same algorithm. It is also called Public-Key Cryptography.

Hash Functions: This type of encryption doesn't make use of keys. It uses a cipher to generate a hash value of a fixed length from the plaintext. It is nearly impossible for the contents of plain text to be recovered from the ciphertext.

USES OF CRYPTOGRAPHY

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

Cryptographic hash functions provide the following benefits to the blockchain:

- Avalanche effect – A slight change in the data can result in a significantly different output.

- Uniqueness – Every input has a unique output.

- Deterministic – Any input will always have the same output length if passed through the hash function.

- Quickness – The output can be generated in a very small amount of time.

- Reverse engineering is not possible, i.e. we cannot generate the input by having the output and the hash function.

Hash functions have a major role in linking the blocks to one another and also maintaining the integrity of the data stored inside each block. Any alteration in the block data can lead to inconsistency and break the blockchain, making it invalid. This requirement is achieved by the property of the hash functions, called the ‘avalanche effect’.

HASHING

The term 'hash function' has been used in computer science for quite some time and refers to a service that compresses a string of arbitrary inputs into a fixed-length string. Cryptographic hash functions have a significant role to play in modern communication technologies. They are a crucial part of cybersecurity and specific cryptocurrency protocols such as Bitcoin.

Hashing is a cryptography method that converts any form of data into a unique text string. Any piece of data can be hashed, regardless of its size or type. In traditional hashing, irrespective of the scale, type, or length of the data, the hash produced by any data is always the same length. A hash is built to act as a one-way function; so you can set data into a hashing algorithm and get a unique string, but if you get a new hash, you can't decode the input data it represents. A unique piece of data will always produce the same hash.

WORKING MECHANISM

Hashing is a mathematical procedure that is easy to execute but incredibly difficult to reverse. The difference between hash and encryption is that the encryption can be reversed or decrypted using a specific key. The most extensively used hash functions are MD5, SHA1, and SHA-256. Some hashing processes are considerably harder to crack than others.

HASHING IN CRYPTOCURRENCY

When a company learns that the passwords of a network have been compromised, it typically means that hackers have obtained the password-representing hashes. Hackers then run the hashes of most used words and combinations of common words and numbers to decrypt some of the passwords that users have saved. The cybersecurity industry is now using the salting mechanism. Salting involves adding random data to the password before hashing it and storing the salt value with the hash. This process makes it more difficult for hackers to use the pre-computation techniques to crack the hashed data they have acquired.

Cryptographic hashing has long played a part in cyber defense and is poised to drive the coming wave of blockchain applications.

PROPERTIES

The perfect cryptographic hash function has the following key characteristics:

- It is foreordained, meaning that the same message will always result in the same hash.

- It’s easy to calculate the hash value for any given message.

- It is impossible to generate a message that yields a given hash value.

- It is difficult to find two different messages with the same hash value.

- A slight adjustment to the message will alter the hash value so heavily that the new hash value will appear completely unrelated to the old hash value, best known as the avalanche effect.

APPLICATIONS

Cryptographic hash functions have a lot of information-security applications, notably in:

- Digital signatures
- Message authentication codes
- Ordinary hash functions
- Indexing data in hash functions
- Fingerprinting
- Detecting duplicate data or uniquely identify files
- Checksums

- Verifying the integrity of messages and files
- Password verification
- Proof-of-work

CRYPTOGRAPHIC HASH ALGORITHMS

There is a mile-long list of Cryptographic hash algorithms, so let's examine just a few of them:

- MD5

MD5 was developed by Ronald Rivest in 1991 to replace the previous MD4 hash function and was listed as RFC 1321 in 1992. Collisions against MD5 can be deliberated within seconds, rendering the algorithm unsuitable for most of the applications where a cryptographic hash is necessary. MD5 generates a 128-bit (16-byte) digest.

- SHA-1

SHA-1 was developed as part of the United States' Capstone Government Project. The original specification now commonly referred to as SHA-0 of the algorithm was published in1993 with the title Secure Hash Standard, FIPS PUB 180, by the U.S. government standards agency, namely the National Institute of Standards and Technology. It was withdrawn shortly after publication by the NSA and replaced by an amended version, published in 1995 in FIPS PUB 180-1 and commonly referred to as SHA-1. Collisions in opposition to the full SHA-1 algorithm can be manufactured using a broken attack, and the hash function should be considered broken. SHA-1 provides a hash intake of 160 bits (20 bytes). Documents may refer to SHA-1 as "SHA," even though this may clash with other regular hash algorithms such as SHA-0, SHA-2, and SHA-3.

- Whirlpool

Whirlpool is a cryptographic hash function developed by Vincent Rijmen and Paul S. L. M. Barreto, who first defined it in 2000. Whirlpool is based on a significantly modified version of the Advanced Encryption Standard (AES). Whirlpool provides a 512-bit (64-byte) hash digest.

- Bcrypt

Bcrypt is a password hashing function, its roots based on the Blowfish cipher, which was presented at USENIX in 1999. In addition to incorporating salt to protect against rainbow table attacks, bcrypt is an adaptive function. Over time, iteration may be increased to make it slower so that it remains resistant to brute-force search attacks, even with increasing computation.

ILLUSTRATION

The potential use of a cryptographic hash can be illustrated using a small example: Jack poses a difficult math problem for Jimmy and claims that he has solved it. Jimmy would like to try it himself, but he’d still like to be sure that Jack doesn’t bluff.

Therefore, Jack writes down his solution, calculates his hash, and tells Jimmy the value of the hash (while keeping the solution secret). Then, when Jimmy comes up with the solution himself a couple of days later, Jack can prove that he had the solution earlier by unveiling it and having Jimmy hash it, and check that it matches the hash value given to him earlier.

CHAPTER SUMMARY

- Cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process.

- Types of cryptography:

  - Symmetric-Key Cryptography
  - Asymmetric-Key Cryptography

  - Hash Functions

CHAPTER 14:

WHAT IS CRYPTOCURRENCY?

Cryptocurrencies are digital (internet-based) assets that are created using cryptography.

Cryptography is making use of code to secure networks, transactions, and digital data, the implementation of which we know as encryption.

Now Cryptocurrency is a combination of cryptography and blockchain technology, so it is ultimately encrypted information given a value and stored and distributed within a blockchain network.

Cryptocurrencies are different from fiat currencies (EURO, USD, and GBP) in the sense that holders assume full control of payments as well as balances. Total control means one does not need a central authority to validate transactions. With fiat currencies, credit card companies and banks usually act as the central authority or gatekeepers on any deal that one is to partake in.

Satoshi Nakamoto is accredited for creating the first cryptocurrency, bitcoin, as well as the underlying blockchain technology in 2008.

Banks maintain a database of people’s money that is usually susceptible to hack attacks. However, that cannot be the case with cryptocurrencies as there is no central authority maintaining records of people's holdings. In addition, transactions on cryptocurrencies are usually conducted in a distributed fashion which makes it hard for hackers to track where funds are moving to and from.

WHAT IS THE RELATIONSHIP BETWEEN BLOCKCHAIN AND CRYPTOCURRENCY?

Remember, blockchain is a technology, and bitcoin and other cryptocurrencies are an implementation of blockchain. They are just products built on it—just as Google or Facebook is an implementation of the World Wide Web (www) and networking. There are many more such implementations or applications built using Blockchain like Ethereum, ripple, stellar, Stratis, etc.

Cryptocurrencies can be envisioned as applications running on top of a cryptographic invention that in this case is blockchain technology. Blockchain is the underlying technology that powers many applications; cryptocurrency is simply one of them.

This implies that blockchain is not the same as cryptocurrency.

DOES BLOCKCHAIN NEED CRYPTOCURRENCY?

I will use another familiar illustration to answer this: A PS5 console and a game disc.

The game disc is an application of the PS5 console, designed to operate when inserted into the console. You can't play the game stored on the disc without the console—it needs it to be able to run at all.

The console, on the other hand, does not need a disc to function, but without the disc, it has little relevance. Imagine having a PS5 console in your house, but no game to play on it.

This is very much the way blockchain and cryptocurrency work. Blockchain does not need cryptocurrency to work, but cryptocurrency is what brought it into relevance. And it is other successful implementations that will keep it in—and even increase its—relevance. Cryptocurrency, on the other hand, cannot be implemented without a blockchain network.

CHAPTER SUMMARY

- Cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process.

- Hashing is a cryptography method that converts any form of data into a unique text string. Any piece of data can be hashed, regardless of its size or type.

- Cryptocurrency is a combination of cryptography and blockchain technology, so it is ultimately encrypted information given a value and stored and distributed within a blockchain network.

- Blockchain is a technology, and bitcoin and other cryptocurrencies are an implementation of blockchain. They are just products built on it—just as Google or Facebook is an implementation of the World Wide Web (www) and networking.

CHAPTER 15:

OPPORTUNITIES IN BLOCKCHAIN

Blockchain expertise is the fastest-growing skill according to the latest skills index and is now one of the hottest in the global job market. Less than a decade ago very few people cared for this technology which has now become a significant career opportunity for professionals.

The demand for people with Blockchain skills is high. Due to its many fields of application, it is looking to hire those who have the skills set to navigate this new technology. Of course, just like with any other fantastic job opportunities, not everyone is cut out for these opportunities. You must have or acquire the skills that set you apart and make an employer want to entrust you with their investment.

Whoever you are, wherever you are, whatever you do, there is a space for you in the blockchain space. Transitioning into the blockchain and web3 sector is one of the smoothest I've seen in the history of job or career transitions. A lot of people share this very limiting belief that they must become some sort of programmers or badass coding genius before they can play or become relevant in the blockchain space.

While it is true that people with these skill sets are highly paid because of the peculiarity of their skills, what is however not true is that you are not relevant here if you do not have those skills. The blockchain space is large enough to accommodate different types of skill and talent. Just take a cue from the use of the internet today. Every industry and sector are ably represented on the internet taking their space. There’s too many non-technical job and career opportunities in blockchain.

We will spare some time to look at some of those industries.

Note: I will only be giving ideas about these careers. There’s still so much due diligence to be done on your part. Read, research, watch videos about your niche and get started.

SOME CAREER PATHS IN BLOCKCHAIN

BLOCKCHAIN DEVELOPERS

The revolutionary blockchain technology opened up a new field of development called the blockchain development. This alone has created job opportunities for developers and tech enthusiasts globally

A developer responsible for developing and optimizing blockchain protocols, crafting the architecture of blockchain systems, developing smart contracts and web apps using blockchain technology are commonly called blockchain developers.

Blockchain developers are in high demand and are well paid due to the peculiarity of their skills. There are endless opportunities for them.

Technical Skills Required to Become a Blockchain Developer

1. *Blockchain Architecture*

A blockchain developer should have an excellent understanding of blockchain, its working, and its architecture.

2. *Data Structures*

Secondly, an in-depth knowledge and applicative sense of data structures is a necessity when aiming to become a blockchain developer.

3. *Cryptography*

Blockchain is a conjunction of data structures and advanced cryptography, hence it is only obvious that a good grasp on cryptography is also required to become a blockchain developer.

4. Smart Contract Development

Smart Contracts have become a huge thing since the release of Ethereum. Ddevelopers striving to get into the blockchain field should definitely learn about smart contract development. This generally entails learning network specific languages like Solidity, viper, Chaincode etc.

5. Web-Development

Web development is a core aspect of a blockchain developer. To become a blockchain (web3) developer, you have to understand web 2 development and know the basics like java, python and the rest.

BLOCKCHAIN WRITERS

If you get online on LinkedIn, you're sure to find tons of writers who already have the term "blockchain writer" tagged to their profile. But don't think that there already being so many writers mean they are enough, and you would be just another writer in the domain. You won't be. Because going by how fast the blockchain industry is scaling, and how rapid the growth of this sphere is, there's a constantly rising demand for quality content. And you, will have a lot of room to create your own mark in the industry.

Being the exceptional technology blockchain is, there's a lot of hype around it, and it's growing exponentially. Owing to this, there is a lot of money flowing around the whole industry. So, if you have the potential, talent, the skill set that people are seeking, you'll be handsomely paid. Given that you've gained some experience to show off and know how to market yourself, blockchain can be one of the highest paying niches for you.

Skills Required to become a blockchain writer.

1. Be a good writer. And if you are a professional writer already, familiarise yourself with the blockchain industry and get started.
2. Consistently write about ICO, news, and start-up projects in the blockchain and

cryptocurrency world on your social media and blog.

3. Take courses on content writing, blockchain and cryptocurrency
4. Read books and magazines about blockchain and crypto.
5. Join blockchain and crypto communities online and make your presence known by consistent engagements.

BLOCKCHAIN/CRYPTO COMMUNITY MANAGERS

Another promising career that is evolving fast in the blockchain ecosystem is community management. Blockchain and web3 is a community sensitive technology. There are no way projects can thrive in this space without communities. For every project created, there is a community and for every community, there will be need for community managers.

There is nothing out of the blues in managing blockchain communities. If you can manage a WhatsApp group as an admin, then you can do this job. All you just need is to expand your knowledge about blockchain and crypto.

Some platforms used for blockchain projects are Telegram, Discord, Slack and Riot.

Telegram, for example, is a stream of consciousness meets forum. It is currently the de-facto standard for hosting communities of blockchain projects. Your management and tracking skills will be very limited but discussions may happen more organically.

Discord, on the other hand, provides incredible framework and structure for moderation. Having been primarily targeted towards gamers, they have channels, integrated voice, and video calls, screen-sharing which make everything easier for both the community and moderators.

Slack and Riot are also used by some crypto communities but haven’t gained enough traction to be considered mainstream options in the crypto world.

Roles and Responsibilities of Blockchain Community Managers

Some roles and responsibilities of blockchain community managers are but not limited to:

- Moderate community channels (Discord, Telegram, etc)
- Share content to social media
- Create video tutorials
- Educate the community
- Curate ideas for growth
- Broaden the community
- Invite friends/family
- Collect feedback (UI/UX, Website, social media...)

- Bug/Hack Bounty
- Connect to press & influencers.

BLOCKCHAIN LEGAL CONSULTANTS

As organizations try to comprehend the adoption of Blockchain into their systems, legal issues always arise. As companies launch this new technology, they are also looking for legal expertise on what considerations to make while investing. They are curious about the implications of their actions, about how to handle their finances, and lastly how to manage their identity.

Also, talking about smart contracts.

In law, contracts cannot be self-executed. Contracts still need the involvement of lawyers, judges or the police to be enforced. Smart contracts which are very important elements in blockchain technology are a direct opposite of this as it helps to simplify business and trade between both anonymous and identified parties, sometimes without the need for a middleman. They share the same set up like traditional contracts but the only difference is that they can self-execute.

Blockchain developers will always need lawyers to function.

As a lawyer who aspires to be relevant in the blockchain sphere, get versatile knowledge about blockchain, get your team together and be up to something meaningful. Your team should consist of blockchain developers, web developers, Python, Java, C++ pros.

EVERYONE CAN PARTICIPATE

Besides the specific roles of professionals working with Blockchain technologies, it is also important that everyone in the organization has a fundamental organization of the Blockchain. Only when everyone has an understanding of the benefits, key capabilities, use cases, and critical success factors, organizations can fully exploit the Blockchain.

Other Connected Roles

- Accountants
- Public Relations
- Marketers
- Crypto journalists

- Managers
- Crypto brokers
- Analysts
- ICO advisors

CHAPTER SUMMARY

As Blockchain technology continues to evolve, so will its professional opportunities. The Blockchain is here with us to stay which means that Blockchain Expertise is to be in high demand for years and years to come. So, whether you are a techie or not, a career in Blockchain is a new and exciting opportunity worth exploring.

BONUS CHAPTER 1:

DEFI AND THE AFRICAN MONEY SYSTEM

DeFi means Decentralized Finance.

It is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies.

A major industry that has enjoyed and will continue to enjoy the benefits of blockchain technology is the finance sector. Safe to say what the finance sector is enjoying is “The First Mover Advantage”. While other sectors are trying to catch up fast and take their place in the technology of the future, the finance sector is taking the front seat. This is so because bitcoin (money) was the first and major successful experiment of blockchain technology.

With blockchain technology, people practically become their own banks. Meaning the banks can be boycotted and at the same time still enjoy all the amenities being provided by the banks and even more.

The most powerful tool of the government is CONTROL and that is what blockchain technology has come to challenge.

With control, the government can put fear in people and toss them in any direction they want them to go.

Blockchain takes control from the government and give to individuals.

When people control their own banks, then the traditional banking system will be of no relevant use.

Africa, being home to some of the fastest growing economies in the world, and with a demographically youthful population, the time has come for the needed disruption in financial services and technology.

Talk of mobile money adoption, Africa is a pace setter with digital transactions accounting for over 45% of mobile money transactions globally serving the unbanked all over the continent.

And in spite of this growth, centralized finance (CeFi) still controls much of digital finance in Africa. This means that banks, government institutions, and other traditional institutions are still responsible for most of the infrastructure through which the digital banking revolution is taking place. This structure is limited, and at a huge disadvantage when it comes to innovation.

With DeFi, people in Africa with adequate access to banking can finally gain access to financial tools such as being provided liquidity, borrowing, lending and saving that will be essential in a growing economic market.

This is possible because with blockchain technology comes DeFi which helps people become their own bank and enjoy all the services offered by traditional banking system seamlessly and more profitably.

DeFi also gives access to crypto loans. A situation where loan is given to a borrower in exchange for his crypto assets.

While DeFi is a liberation tool to the people of Africa, there is still a wide knowledge gap as most Africans have no idea about decentralized systems, never mind how they work.

There is still so much sensitizing to be done and that is where blockchain education comes to play. Without education, there can never be adoption.

BONUS CHAPTER 2:

WHAT EVERY CRYPTO TRADER SHOULD KNOW

As a blockchain educator, one of my key job descriptions is to provide blockchain education and training to blockchain beginners and help people position well in taking their place on the space without holding back obvious facts. With Africa being a global leader in crypto trading, it is crystal clear that crypto trading (precisely bitcoin) was what introduced us to blockchain technology. And in fact, bitcoin was introduced to the larger African through the global Ponzi scheme, MMM.

What do you expect of a continent where practically everyone has to fend for themselves and take care of their well-being? Where most people have potentials but there's limited platform for expression? They jump at everything that can fetch them fast and easy money not minding whether it will have any negative consequence or not.

This is not to downplay or discredit crypto trading. I started off my journey on this path as a crypto trader myself and I still do. But there's more. Trading is just an aspect of the whole ecosystem.

As at present, only a handful of traders have an understanding of blockchain technology.

The essence of crypto is not just for it to be traded, buy low and sell high or chase pumps and dumps. Limiting crypto to just these will be too unfair on the disruptive technology called blockchain and with that kind of mindset, Africans will not fully harness the full potentials of the technology.

Crypto is much more than just a money-making scheme. It is a movement. Crypto is here to change every area of our lives.

Crypto is the mode of transaction in web3. What this means is simply this: going forward, crypto is the reward for every value that will be created on the blockchain. Reward will be earned in crypto.

There is a trend forming and it is forming fast. It is the Web3 (Metaverse). We need to catch this trend and get busy to understanding the technology behind crypto which is blockchain.

Would you rather chase the bubbles now, make the peanuts and be nowhere to be found on the space in 10years time?

Or would you sit down, learn the technology and build systems that will create streams for people and continue to stay relevant in the future?

In every trend, system builders become the real deal eventually.

If you cannot build, align and collaborate with builders. Join someone who is seeing a bigger picture about blockchain today. We know how those kinds of stories end eventually.

ABOUT THE AUTHOR

Adeshina Ajayi is the Chief Executive Officer of Digital Focus. A Digital company focused on Blockchain education and awareness.

He is a leading financial literacy advocate and enthusiast, highly competent Blockchain expert with over ten (10) years of experience in Leadership Management and four (4) years of accomplishment in Blockchain Technology space for social impact, Human development and financial capacity building.

Adeshina is an alumnus of the prestigious London Graduate School (LGS) where he bagged a certification in Management Specialist with distinction in Time Management. He was certified a blockchain expert by the prestigious Blockchain Council after he graduated with a distinction.

He is happily married to his beautiful Wife Adedayo and the union is blessed with two boys Brian and Ethan.

The digital world is here to stay and there is a lot of untapped resources on it. Blockchain Technology is a major disruptor in the digital space and it is the technology of the future. To tap into the resources and opportunities that this technology provide, there is the need for education and awareness. These two are the purposes of this book. To educate the reader and create an awareness about blockchain technology so that people can make informed decisions and take their place in the future wealth technology.

ISBN 9789789959068
9 789789 959068

PUBLISHED BY:
ACE world Publishers

DIGITAL FOCUS