CONSPECTUS OF BLOCKCHAIN

Dr. K. Hema Shankari

Jupiter Publications Consortium
www.jpc.in.net

Conspectus of Blockchain

Author:

Dr. K. Hema Shankari

First Edition March 2021

ISBN 978-81-947069-1-5

9 788194 706915 >

ISBN: 978-81-947069-1-5

Pages: 204

Price: 350/-

Publisher & Imprint:

Jupiter Publications Consortium

22/102, Second Street, Virugambakkam

Chennai, Tamil Nadu, India.

Email: director@jpc.in.net

Copyright Disclaimer

Publisher's Address:

Jupiter Publications Consortium
22/102, Second Street, Virugambakkam
Chennai, Tamil Nadu, India.
Email: director@jpc.in.net

Title Verso

Title: Conspectus of Blockchain

Author's Name:

Dr. K. Hema Shankari

Published By:

Jupiter Publications Consortium

Publisher's Address:

22/102, Second Street, Venkatesa Nagar, Virugambakkam
Chennai 600 092. Tamil Nadu, India.

Printer's Details:

Jupiter Publications Consortium

Edition Details: I

ISBN: 978-81-947069-1-5

Preface

Several people use the term "Conspectus of Blockchain" to refer to a variety of items. They also mention cryptocurrency or digital currencies, the Ethereum Blockchain, or smart contracts. The irony is that some people often misuse ‘Blockchain' because many people have been misled by the term 'Blockchain' and its terminology and terminology. Both applications, though, have one thing in common the underlying distributed ledger technology. Instead of being held on a central database, transactions in distributed ledger technologies are copied and saved by individual computers on the network.

Although Blockchain technology has progressed faster than predicted, exact specifics have only recently reached well-known developers and technophiles. Several websites and devoted sites are now appearing to explain the whole technology and developments around it. However, it seems that there is already a need for a comprehensive guide that familiarises and contrasts the overlapping terms and terminologies associated with blockchain technology. We (Authors) want to create a comprehensive guide in this regard, one that covers all the foundations of Blockchain technology and popular technologies, and terminologies associated with it.

It is a must-read for those interested in learning more about blockchain technologies. We did our best to organise the topics so that developers and technocrats could easily navigate them and enjoy them. However, let us keep in mind that this book does not include anything we will need to get started with blockchain; instead, it is a starter kit. We are using this as a starting point to learn more about Blockchain technologies and expand our knowledge base.

- Dr K. Hema Shankari

This Page Intentionally Left Blank

Foreword

Blockchain technology has advanced since Satoshi Nakamoto first proposed it in 2008. There is much buzz about the phrases "bitcoin," "blockchain," and "cryptocurrency" Startups and policymakers have finally begun to bring in the effort using blockchain technologies. They will do so in the future as well. Blockchain technology is discussed by the author in-depth in this book, which details how readers will take advantage of its ability.

After reading this book, conceptually, we understand that the blockchain starts off to build positive impact and disruptive technologies. However, we are now exploring all the potential blockchain technology provides. In the beginning, blockchains were created to enhance Bitcoin's cryptocurrency record-keeping mechanism. Nowadays, though, they are being applied to store records of different forms of applications. If we did not have many intermediaries, several of the things we all rely on, including money flows, voting, land records, intellectual property, and identification, would not work. These outdated structures are now being rendered redundant using blockchain apps. If the software has been applied, it will act as a trustworthy record-keeping device. In contrast, the coded laws will serve as the mediators.

The author discussed blockchain technology rudiments comprehensively in this book, and the student should know next or nothing about it. Additionally, it provides the reader with an understanding of the significant gaps in blockchain applications and how and why these technologies operate. After going through this book, I understand that the readers who completed reading this book would have a clear grasp of the technological gaps in two defined cases and will feel more positive when explaining them. The reader can also hear about the intrinsic drawbacks and weaknesses of blockchain technology.

I wholeheartedly appreciate Dr K. Hema Shankari, who is presently working as an Associate Professor in the Department of Computer Application in Women's Christian College (Self-financed section), Chennai, for authoring this book as per the contemporary requirements for Undergraduates and Postgraduates that shall throw more light on understanding the basics of Blockchain technology. I wish her all success in all her academic and research endeavours.

Mr. N. Tamilselvan
Architect Technology
Cognizant Technology Solutions
United States of America (USA)

Acknowledgment

The scripture says, "For the Lord gives wisdom; from his mouth come knowledge and understanding". First and foremost, I thank the Lord Almighty for giving me the knowledge and wisdom to write this book.

My sincere thanks to **Dr. Lilian I Jasper**, Principal, Women's Christian College, who has been a constant support in all my endeavours.

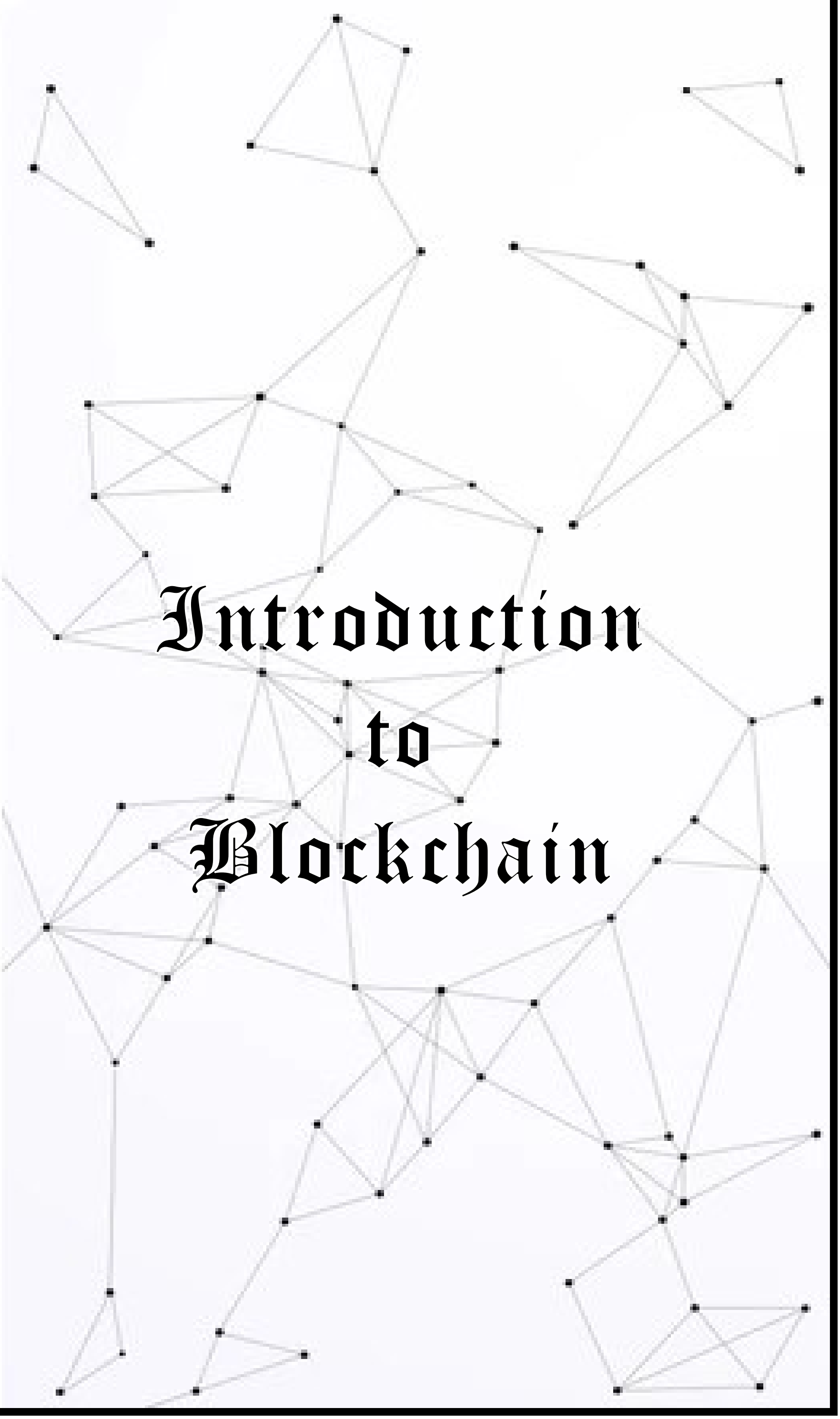
I thank **Mrs. D. Sylvia Mary**, Head of the Department, Department of Computer Applications, Women's Christian College (WCC) and all my colleagues for their encouragement and support.

A special thanks to my family. Words cannot express how grateful I am to my mother, **Mrs. K. Banumathy**, and my father (late), **Mr. A. U. Karmegam**, for the sacrifices they have contributed towards my growth. I express thanks to my beloved husband, **Mr. S. Prabhakar**, and my son **Mr. Freddy Samuel Prabhakar** and my daughter **Ms. MiraclelinYuketta Prabhakar** for their untiring efforts constant support in publishing the book successfully.

- **Dr K. Hema Shankari**

This Page Intentionally Left Blank

Table of Contents

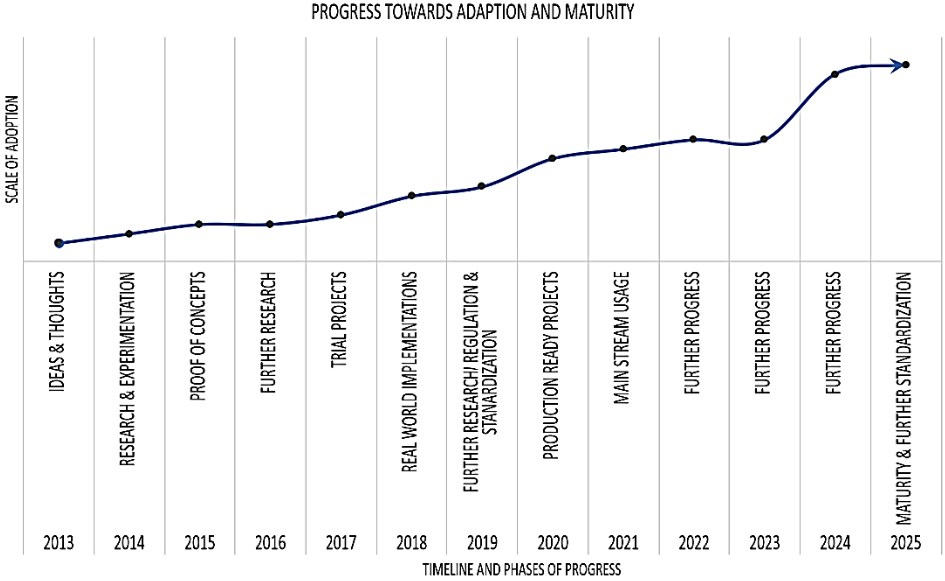


Introduction to Blockchain

The growth of blockchain technology

Our technological society was exposed to a new notion with the advent of Bitcoin in 2008, which is currently expected to transform civilization. It promises to influence any industry, including financial sector, economy, media, law, and arts, but not limited to them. Some define Blockchain as a transition, whilst another school of thinking argues that it would be more incremental. It would take several years for Blockchain to attain any functional advantages. This idea is right, but as per the technologist's view, the transformation by now started. As its transformative ability has now been thoroughly recognized, many leading companies worldwide are now writing a proof of concept using blockchain technologies. Some companies, however, are still in the preliminary stages of exploration. As technology matures, they are projected to advance more rapidly. It is a technology that still has an impact on existing systems and has the potential to alter them at a simple stage. Let us consider the past few times. We recall that in 2013, concrete concepts indicating blockchain usage in fields besides cryptocurrencies started to emerge.

Cryptocurrencies became the main application of Blockchain during the period, and several new coins appeared. The following figure exhibits an exhaustive overview of blockchain technology's year-wise development and adaptation pattern. Years displayed on the x-axis indicate the range of time in which a given blockchain technology process falls. Each period has a name that defines the activity, represented on the x-axis, starting with the thoughts and ideas period, and progressing to sophistication and further standardization. The y axis depicts the level of service, engagement, and approval of blockchain technology. According to the graph, Blockchain will evolve around 2025 because of many users.



The previous graph indicates that, aside from cryptocurrency, Concepts & thoughts appeared in 2013 relevant to other applications of blockchain technologies. In 2014, some development and experimentation began, leading to proof of concepts, additional research, and full pilot projects between 2015 and 2017. We are going to see REAL World Applications in the ensuing years. E.g., the Australian Stock Exchange (ASX) is the first organization to use blockchain technology to replace the clearing and settlement system. Several projects are currently underway to replace existing structures.

During the year 2021, further research and other implications in the governance and standardization of blockchain technology are set to be carried out. Moreover, starting in 2021, production-ready projects and off-the-shelf products based on blockchain technology will be eligible. By 2021, blockchain technology is expected to be widely used—the changes in blockchain technology sound eerily like the internet dot-com boom of the late 1990s. More development is set to continue, as well as the evolution and maturation of blockchain technologies. The software could eventually be mature enough to be used daily by 2025. Please keep in mind that the diagram's timelines are not set-in-stone and can change since it is difficult to predict when blockchain technology will evolve. This graph focuses on recent advancements and the current climate of research, understanding, and enthusiasm for this technology, showing that blockchain technology is expected to grow by 2025. The use of blockchain technology has exploded over the last few years. Previously dismissed as simply geek money or something not worth investigating from a cryptocurrency standpoint, the world's biggest companies and organizations are already studying Blockchain. Adapting and experimenting with these equipment costs millions of dollars. It is evident from the European Union's latest actions, which announced plans to increase funding for blockchain research to nearly EUR 340 million by 2021.

Distributed systems

Understanding distributed systems become essential for understanding blockchain technologies since Blockchain is fundamentally a distributed framework. It is a ledger that is distributed, centralized, or self-contained. A blockchain is intended to be a decentralized network that is widely used at first. It can be thought of as a system of properties of both independent and distributed paradigms. It is a collaborative, decentralized framework.

Distributed systems are indeed a form of computing in which two or more nodes work together in a coordinated way to achieve a common purpose. It is designed to be used by end-users as a single logical platform. E.g., Google's search engine is based on a vast, distributed architecture. To a customer, though, it seems to be a single, interconnected network. A node may be defined as an independent player in a distributed system. Each node can send messages to and from each other and receive messages. Nodes and have memory, and a CPU may be truthful, unreliable, or malicious. A node that displays irrational behaviour is referred to as a Byzantine node after Byzantine Generals problem.

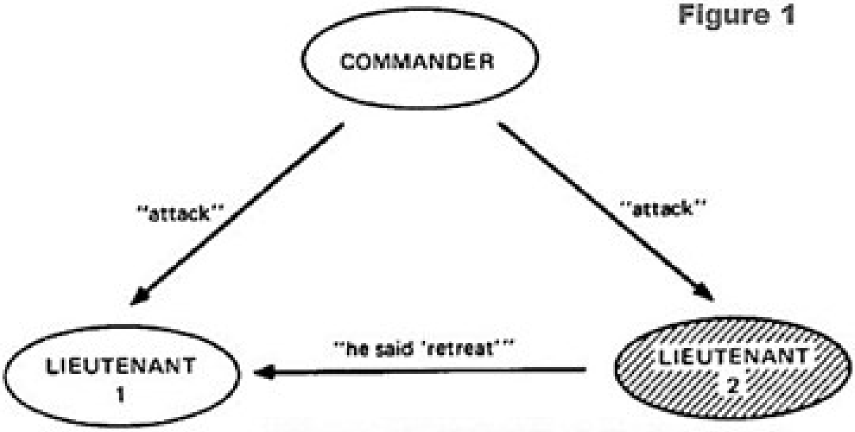
BGP — Explained as a fictitious historic incident

Let us assume that the Byzantine Army, called Grand Eastern Roman Empire, has captured a particular region. However, within the area, there is fierce opposition. The Byzantine army encircles the city. Each division of the army has its general. The generals use only messengers to coordinate with each other and their respective division's lieutenants.

All generals or commanders must accept either of the two plans of action. The right moment to strike all at once, or, whether we are up against much opposition, the precise moment to withdraw all at once. The army would not be able to maintain its position indefinitely. Suppose the assault or retreat is not made in absolute intensity. In that case, that can only signify one thing: a severe failure that is unacceptable.

It would be an easy answer if both generals and/or messengers were reliable. Various messengers and a few generals/commanders are found to be traitors. However, they are either informants or rival groups. An acceptable risk was there that they would not obey instructions or may deliver the wrong letter. The army has a low degree of public confidence.

Figure 1



The one with stripes is the traitor because of which a consensus cannot be reached

1 commander and 2 Lieutenants and just 2 types of messages Consider just a case of 1 commander and 2 Lieutenants and just 2 types of messages- ‘Attack’ and ‘Retreat’.

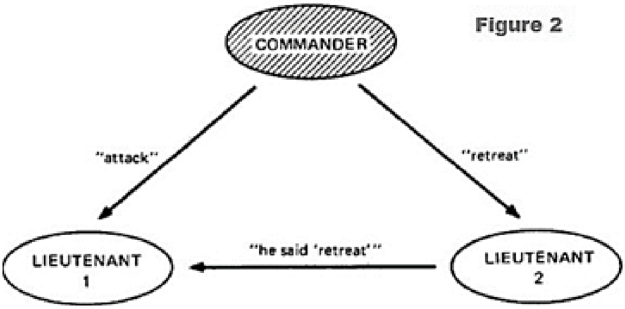


Figure 2

Figure 1 — Lieutenant 2 is an accomplice who deliberately transfers the message to Lieutenant 1. In Figure 1, Lieutenant 2 is a traitor who alters the letter that is supposed to be sent to Lieutenant 1. Lieutenant 1 has received two reminders and is uncertain on which one to follow. Lieutenant 1 is assumed to follow the Commander due to the army's rigid structure. Even if Lieutenant 2 is a traitor, coercion impoverishes 1/3 of the force, resulting in chaos. What if the Commander, on the other hand, is a conspirator? (as described in Picture 2). At Present, two-thirds of the army has taken the wrong order, and defeat is a foregone conclusion.

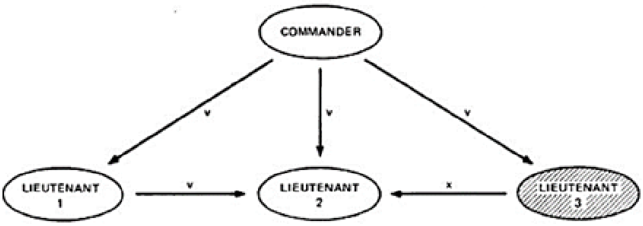


Figure 3

The one with stripes is the traitor because of which a consensus cannot be reached

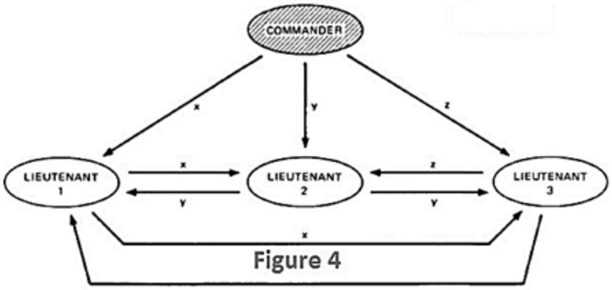


Figure 4

One commander and 3 Lieutenants, and just three types of messages

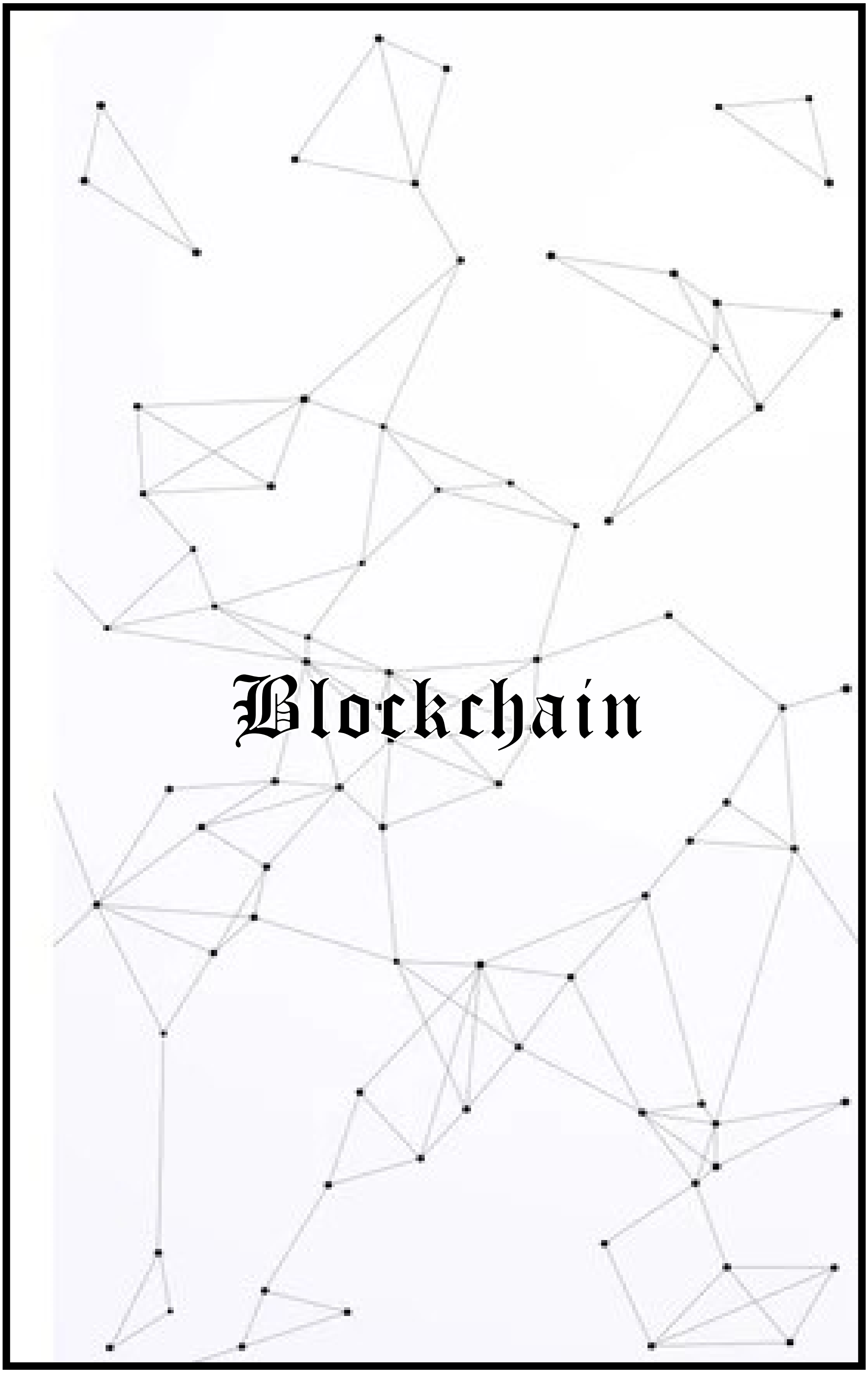
In Figure 3 and Figure 4, we have just added 1 more Lieutenant and 1 more type of message (Let us say the 3rd message is ‘Not sure’).

The problem in deciding for all the Lieutenants and the Commander is immediately enhanced. Consider how quickly the number of Lieutenants grows as there are many of them.

This is BGP for short. It can be seen in any distributed network. Since there is no real 'General' or server in the Bitcoin network, it is much more complicated. The hierarchy of all members or nodes ('Lieutenant') is precisely the same.

Any message sent between the nodes must be agreed upon by all participating nodes. The network will not be corrupted and can survive this 'Attack' even if a group of nodes or even the communication they send is corrupt. In other words, any message sent in the network must be agreed upon by the whole network. The consensus is the term for this kind of agreement.

Blockchain



Blockchain

In 2008, under the pseudonym Satoshi Nakamoto, a pioneering paper titled Bitcoin: A Peer-to-Peer Electronic Cash Infrastructure was published about peer-to-peer electronic cash. It pioneered the 'chain of blocks' concept. The world was not aware of Satoshi Nakamoto's real name. However, he was engaged in the Bitcoin developer community till 2011, after launching Bitcoin in 2009. He then turned over the development of Bitcoin to its leading developers and vanished. There has been no contact of any sort from him since then, and his life and identity are veiled in mystery. Over the years, the term chain of blocks developed into the word Blockchain. Blockchain technology, as mentioned earlier, integrates a variety of applications that could be employed in different divisions of our economy. Significant changes in financial transactions and settlements' efficiency result in good time and cost savings, especially in the finance sector.

Blockchain defined

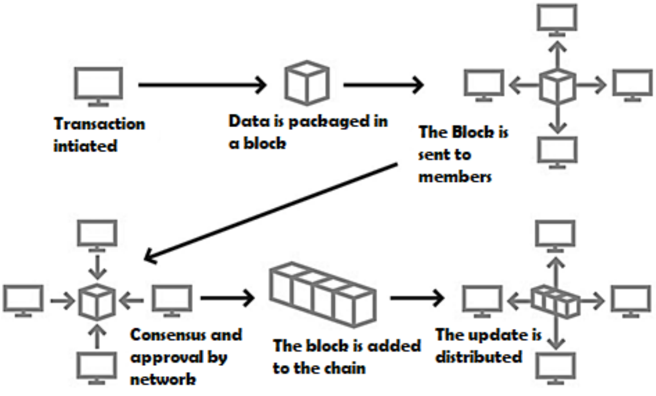

Transaction intiated
Data is packaged in a block
The Block is sent to members
Consensus and approval by network
The block is added to the chain
The update is distributed

Figure 5: Blockchain defined diagram

Layperson definition: Blockchain is indeed a perpetual growing, stable, decentralized record-keeping mechanism in which each recipient of the data keeps a copy of the documents, which could be changed with the condition that both parties agree to a transaction by updating it. A simple flow diagram of Blockchain defined is shown in Figure 5.

Technological definition: Blockchain is a cryptographically secure, append-only, irreversible (complicated to modify) peer-to-peer, distributed ledger that can just be changed by consensus or agreement of peers. The more in-depth details with appropriate meanings are discussed in the following chapters with a glance of all keywords with definitions one by one.

Peer-to-peer

As in the technical description, Peer-to-Peer is considered as the first keyword. This suggests that the network does not have a central administrator, and all members speak individually to each other. This property enables cash transfers to be freely traded between peers without the intervention of third parties, for instance, 'a bank'.

Distributed ledger

Furthermore, analyzing theoretical concept shows that 'Blockchain is a distributed ledger', which essentially implies that a ledger is delivered amongst 'all peers in the network' across the network. Many of the peers on the network own a complete copy of the ledger.

Generic elements of a blockchain

Before we go any farther, let us have a brief look at how a blockchain works. Whenever we find ourselves introducing a review to the different subsections, It is an excellent guide to understand the mechanism's overall construction. Certain, deeper layers will be covered. For example, in later pages of the book, the subject would address other unique blockchains such as Hyperledger Virtual Fabrics. It describes distributed virtual networks within hyperledger to direct-fabric technologies. With the help of the following illustration, the layout of a regular blockchain-based validator and member node six can be seen in Figure 6. Any use case of the blockchain that we can see below has at least one specific elements from a blockchain. Elements such as open-source and decentralized that we commonly appear with Blockchain

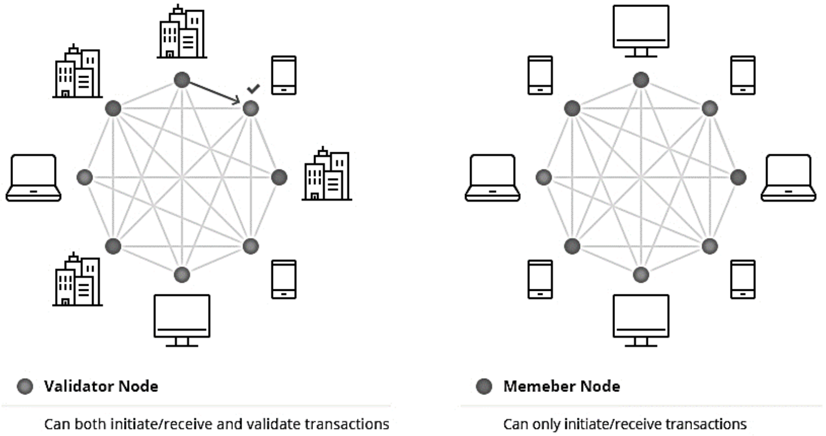

● Validator Node
Can both initiate/receive and validate transactions
● Memeber Node
Can only initiate/receive transactions

Figure 6: Architecture of a Common blockchain with nodes

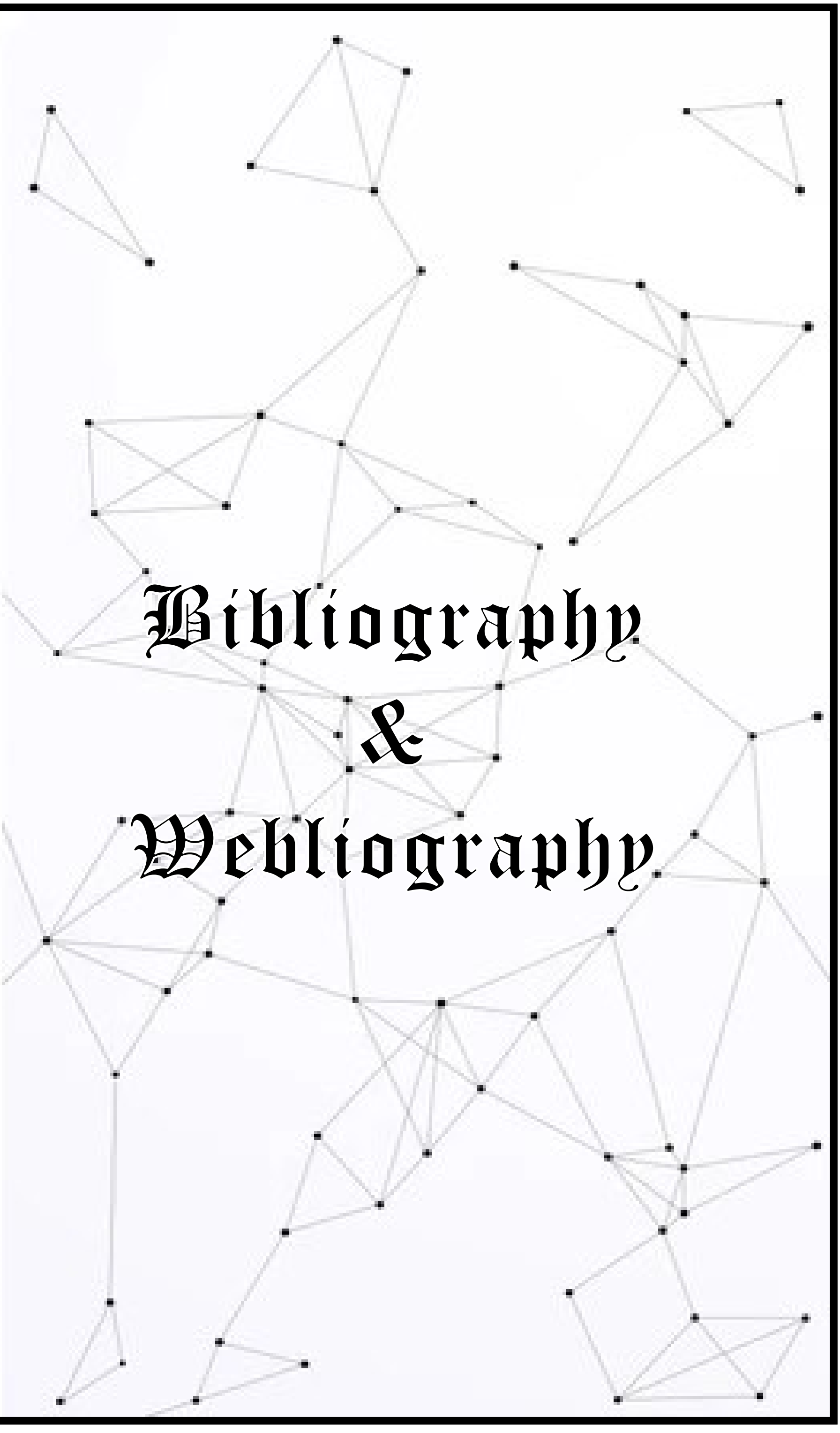
Address: It is a unique identifier utilized to denote senders and receivers in a blockchain contract. In practice, most often, public keys are derived from their corresponding private keys. While the same user will repeat addresses, the addresses themselves are unique. A single user can never use the same address and generate a new address for each transaction. It will only be available at this newly established address. Bitcoin is a fictitious currency. End-users are typically unknown, but some research has shown that they can be easily identified by removing Bitcoin users' anonymity. To prevent transactions from being linked to the usual owner, users can generate a new address with each transaction, thereby avoiding identification.

Transaction: A transaction is the fundamental unit of a blockchain. A contract is a value transfer from one address to another.

Block: A block contains multiple transactions and other elements, including the previous block's hash pointer, timestamp, and nonce.

Peer-to-peer network: A peer-to-peer network is made up of networks and is a network topology in which all connected peers can send and receive messages.

Scripting or programming language: Scripts or programs perform different operations on a transaction to allow several tasks. Transaction scripts are predefined in a language called



Bibliography & Webliography

Bibliography

1. Drescher, D. (2017). Using the Blockchain. In *Blockchain Basics* (pp. 223-233). Apress, Berkeley, CA.
2. Judmayer, A., Stifter, N., Schindler, P., & Weippl, E. (2019). Blockchain: Basics. In *Business transformation through blockchain* (pp. 339-355). Palgrave Macmillan, Cham.
3. Julie, E. G., Nayahi, J. J. V., & Jhanjhi, N. Z. (Eds.). (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. CRC Press.
4. Laurence, T. (2019). *Blockchain for dummies*. John Wiley & Sons.
5. Morabito, V. (2017). Business innovation through blockchain. *Cham: Springer International Publishing*.
6. Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Apress.
7. Stratopoulos, T. C., Wang, V. X., & Ye, J. (2020). Blockchain technology adoption. *Available at SSRN 3188470*.
8. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".
9. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Webliography

1. Expert, B. (n.d.). Blockchain Expert. https://www.blockchainexpert.uk
2. (n.d.). Medium. https://medium.com
3. (n.d.). no title. https://users.cs.fiu.edu
4. (n.d.). Packt | Programming Books, eBooks & Videos for Developers. https://www.packtpub.com
5. (n.d.). Solidity — Solidity 0.8.2 documentation. https://solidity.readthedocs.io
6. (n.d.). TechBlog. https://shyamtechno.blogspot.com