Future of Web3 Education

WHAT IS BLOCKCHAIN?

Blockchain is literally a chain of blocks, with each block containing certain data. The blocks are chained in such a way that it is not easy to break the chain. Blockchain was first introduced through a white paper authored by Satoshi Nakamoto [Link 3]. While the concept of a distributed ledger existed before, this paper introduced bitcoin cryptocurrency which has blockchain as the underlying technology. Let us look at a few formal definitions of blockchain before understanding these concepts.

Harvard Business Review defines blockchain as “An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.”

Merriam Webster Dictionary defines blockchain as “A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network or the technology used to create such a database.”

Blockchain can also be defined as “A system in which participants of a peer-to-peer network maintain distributed ledger that is secure, practically immutable and auditable.”

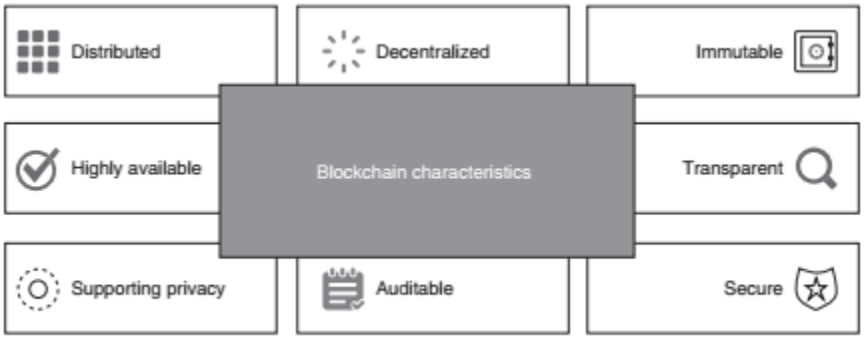
Let us understand few terms relevant to this technology.

1. **Parties/Participants**: Organizations or systems that participate in the network for reading or updating the data.
2. **Open**: Protocols and details of working are not closed or proprietary. Blockchain protocols are published and documented for everyone’s consumption.
3. **Distributed ledger**: A log of transactions that is same from all the nodes connected and synced with the network. In simple terms, every participant has the same copy of the log they all are maintaining together.
4. **Peer-to-peer network**: A network in which participants are connected to each other than a central server of a hub.
5. **Permanent**: The ledger that is probabilistically impossible to change once it is agreed by the participants.

BLOCKCHAIN CHARACTERISTICS

Before jumping into details, let us attempt to understand the concept of blockchain through an analogy. Assume that there is a social media group of fans of a popular cooking show. The fans watch the show that is telecast every Sunday, try the recipe out over the next few days, and then discuss nuances and their experiences. The recipe show, appreciating the passion of followers, has joined the group and places the recordings of the show on the social media platform. Individuals cannot delete what they have posted, and fans get a copy of the chat on their mobile. If a new fan is to be added, a member proposes and everyone votes to accept or reject the proposal and also to decide who will get incentive to add the new member. There is no administrator or hierarchy. If a fan posts a wrong recipe, then there can be another post with

the updated recipe, but the log cannot be changed. Everyone sees the same log, so there is much more transparency in the information shared. Loosely, blockchain is very much like this chat; transparent, peer-based, immutable, and consensus-driven.



Blockchain characteristics.

After understanding what a blockchain is, let us try to understand the characteristics of blockchain. This will help us appreciate the value that blockchain brings to the table.

1. **Distributed**: The single constant theme in blockchain is collaboration. For collaboration to happen, there has to be more than one system. Blockchain processes and stores data in multiple participants and by nature, blockchain is a distributed system.

2. **Decentralized**: There is no single decision-making authority that exists in blockchain network; the decision to store or reject certain data is taken collectively by participants based on preset rules.

3. **Highly available:** Distributed and decentralized nature of blockchain networks helps ensure consumers that the network always has a node available to serve the requests; this is what makes blockchain highly available.

4. **Immutable:** As discussed above, in blockchain, data is stored in a chain of blocks. If the chain is designed in such a way that it cannot be broken, the data inside the blocks of chains cannot be modified. This non-modifiability is what makes transactions performed in blockchain networks immutable.

5. **Transparent:** In a blockchain, all the participants have a copy of ledger entries. Entries to the ledger are created by preset rules that are defined at network configuration. This sharing of data and logic encourages transparency in blockchain.

6. **Auditable:** Blockchain does not only have current state, but the entire journey of journal or log of how the state has been reached. The log is available for each node in the system. This makes activities happening on blockchain auditable.

7. **Secure:** Blockchain extensively utilizes encoding and encryption mechanisms for transaction creation, broadcast, and storage. Blockchain, if, design does not encourage

use or participation of unauthorized nodes to store any information that can help identify a key or participating node in the real world. The distributed nature of blockchain creates multiple barriers for hackers to find ways. To be more participants, more secure and resilient the network.

8. **Supporting privacy:** Blockchain does not identify individuals with identifying information in its design. Information about transactions initiated by party A with party B, for whom it is not enough to understand the transaction, can make blockchain secure.

9. **Democratization of trust:**

   The trust equation states that trust in blockchain networks is assured by participants with no middlemen as in traditional systems. The trust equation is what helps ensure privacy, security, and privacy makes blockchain a dependable system, credibility cannot be acquired, as entities, a way must be implemented like regulations around the same, and trust ensures the credibility of the entire framework. In this model, trust is defined by code and ensures the participation of any trust in a democratic but is “appointed”.

   On the other hand, blockchain takes a radically different approach to become trustless. Blockchain participants or nodes can agree and even rule or choose a decision-maker transparently for each transaction. This means that anyone can participate in the system as a trustworthy peer is chosen each time from peers; the chosen node is not “appointed”.

Blockchain use case types			
Provenance	**Payments**	**Transaction ledger**	**Identity**
• Restaurant giving customers view of journey– a fish has taken to reach customer's plate • Pharma companies detect counterfeit products • Farm to cup journey of coffee	• Funds transfer using cryptocurrency • Triggering claim settlement for parametric insurance • Issuing loyalty rewards to customers based on type of activity and transactions	• Storing health history of individuals supporting borderless healthcare • Supporting Know Your Customer use cases for changes to demographics • Partial ownership of high value assets such as real estate	• E-consent management for end users • Self Sovereign Identity based on zero-Knowledge proof • End user controlled data sharing or data sell

Blockchain use cases.

While payments use cases is where the blockchain journey started, evolution of blockchain to execute code based on certain conditions has created numerous possibilities in area of loyalty management, insurance claim settlement, etc.

Blockchain, when viewed as just ledger of non-financial transactions with feature of immutability and transparency, creates a whole new dimension of use cases. For instance, patient health

history can be captured to identify events where detailed health reports can be stored off-chain and can be retried on need basis. Similar use cases related to partial ownership of high-value assets, assisting regulators in implementation of Know Your Customer (KYC) requirements, supporting insurance subrogation, all fall under this category.

The last area is management of identities through blockchain technology. Individuals have become significantly aware and concerned about sharing their private information. They have also realized that they need to have control over data and they would want to get benefited for organizations that use their data. These not only give control to end user for data belonging to them, it also creates new avenues for organizations to management consent and collect data through ethical and quality sources. End users can also monetize their data at a rate and value that they feel is rightful.

HISTORY OF BLOCKCHAIN

Humanity has been using distributed ledgers around 1000 years ago. While blockchain as we know it is a new concept, the idea of having a distributed ledger was discovered long back. On the Yap islands of Western Pacific Ocean, native islanders used a stone currency named Fei or Rai. They used large stone disks, usually 12 ft in diameter. These stones were large, heavy, and difficult to move. Instead of moving the stone, people kept in mind what transaction had happened. It is said that even when the stone was submerged or lost, people could still transact the stone based on a mental map they had. This mental mapping is very much conceptually similar to the theory of who owns what; it was similar to the distributed ledger and each had their own copy.

Talking specifically about blockchain we know today, in 1991, Stuart Haber and W Scott Stornetta ideated using a system where document timestamps could not be tampered with using cryptography. The next year, in 1992, Stornetta, Bayer, and Haber explained the use of Merkle trees for improved efficiency working with these chain of blocks. As mentioned earlier, in 2008, Satoshi Nakamoto proposed a peer-to-peer transaction cash system using blockchain, where a method was proposed so that blocks can be added to the chain with all participants being given a level playing field. It should be noted that Satoshi introduced electronic currency based on blockchain but blockchain is much more than cryptocurrency.

Organizations started developing and piloting use of transactions on bitcoin. From 2014 through 2015, major players in this technical domain, such as Hyperledger, Ethereum, and R3, were introduced. From 2016 onward, these have sustained steady growth and adoption, building smart contract ecosystems, and sustaining decentralized applications, among other things. The technology is continuing to move from decentralized currency uses to distributed computing to decentralized storage. A number of organizations are creating their own storage, identifying and applying new use cases and helping the blockchain platform mature.

SKILLSETS REQUIREMENTS

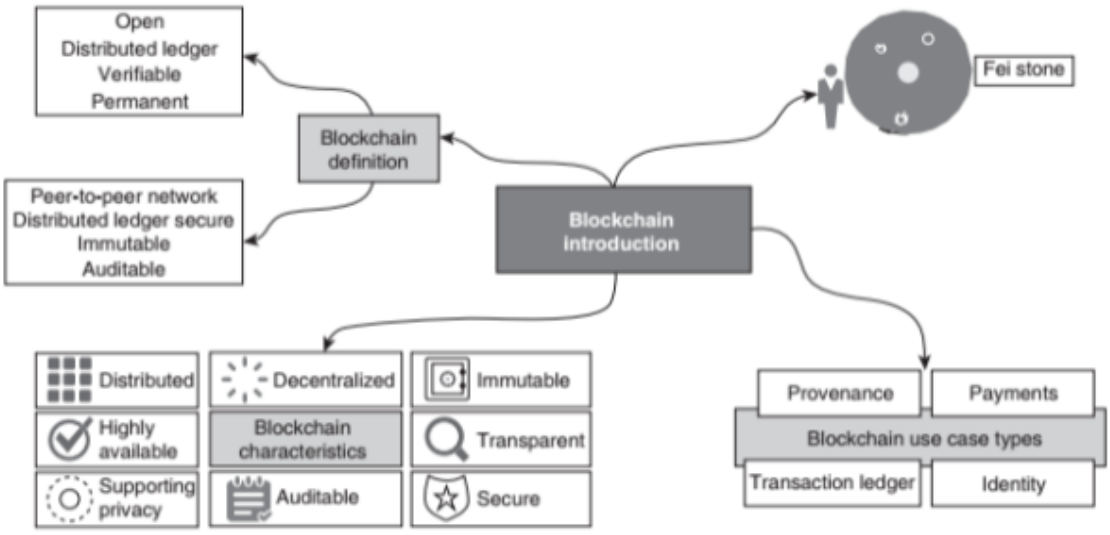
Before closing on this chapter, let us understand at a high level, expertise required to realize solutions using blockchain technologies. This expertise will be articulated in terms or roles that individuals would need to play and skills that each of these roles would require.

At a high level, there are three roles that support solutions on blockchain in enterprise environments—blockchain consultants, blockchain solution architects, and blockchain developers. Of course, there are a few more but in summary a large part is participating to develop and govern how blockchain solutions impact software development. Those skills have not been discussed in this book as they are not within its scope. Also, blockchain is a software system and runs in a software environment like other applications.

Blockchain consultants are professionals with industry experience and very good knowledge of the domain in hand. Consultants are supposed to be proficient and comfortable and need to be adaptable and proficient in three different industry-specific solutions. Consultants need to know blockchain concepts, limitations, risks, and different blockchain platforms along with their strengths and weaknesses. Blockchain consultants help identify industry-specific problems that can be solved using blockchain and then conceptualize business cases that can convince stakeholders to invest in blockchain solutions.

Blockchain solution architects are software professionals with industry experience in development in Java, JavaScript, and other open source technologies. More than this, professionals should have previous architecture experience with enterprise systems and hunger to learn and experiment with new technologies. Blockchain solution architects design blockchain solutions, advise business on possible solutions, and help developers through the processes. Another important role of blockchain architects is to help stakeholders who can make key decisions on choice of technologies and tools.

Blockchain developers build meaningful blockchain solutions for end users. These need to be full stack developers who can turn around solutions in a quick time frame with quality code. These developers should be familiar with API calls for enabling mainstream software technologies. Knowledge and JavaScript would be the minimum language for developing code on blockchain have similarity to JavaScript.



Introduction: chapter mind map.

TEST YOURSELF

1. What is blockchain?
2. List the characteristics of blockchain technology.
3. List five different scenarios where blockchain can be helpful.

ASSIGNMENTS

1. Prepare a short note on how the blockchain is different from bitcoin.
2. Prepare a one-page point of view on "Challenges that discourage organizations to collaborate in the current landscape and how blockchain can help circumvent these challenges."
3. Identify different blockchain platforms and create point of view on their strengths and weaknesses.