



Chapter 2

Blockchain and Bitcoin Fundamentals

Chapter Introduction

In this chapter the coverage is specifically focused on ensure the required baseline knowledge before proceeding to the objective coverage. We must ensure we know important facets of blockchain fundamentals and what Bitcoin is.

This chapter will cover what the exam will be testing your around knowing the important fundamentals of blockchain, Bitcoin and basic terminology as well.

CHAPTER OVERVIEW

In this chapter you will learn:

- ☐ What is a blockchain?
- ☐ What is Bitcoin?
- ☐ Blockchain Terminology
- ☐ Technology behind blockchain
- ☐ Summary
- ☐ Practice Questions and Answers



*Blockchain or
Bitcoin?*

Understanding Blockchain and Bitcoin



LET'S DISCUSS BLOCKCHAIN

- Topic – What is a blockchain and Bitcoin?

In this topic the focus on what a blockchain is and cover the brief history of blockchains.

The main objectives you will learn about is

- What is a blockchain
- What is Bitcoin
- Why is the history so important to understand?
- Comparing blockchain to Bitcoin.
- Terminology to know for the exam.



A blockchain is a globally shared data structure, with a transactional backend database that is cryptographically secure

Blockchain Overview

Simply put technically, a blockchain is a globally shared data structure, with a transactional backend database that is cryptographically secure. However, I will be defining this “blockchain” in three approaches.

Blockchains are all about trust in the technology and removing third parties or intermediaries.

A blockchain is a truth machine because of the implementation of the technology used, and this implementation of the ledger maintains the truth since the ledger is an immutable record of trust.

Immutable is a key word meaning that the blockchain transactions (ledger entries) can not be modified or deleted (Integrity).

However, blockchains are frequently confused with a database for example and I really don’t believe one definition fits all audiences, so I took the initiative to expand on the definition.

Defining a blockchain

The definitions are aligned to the specific audiences that are interested in the possibilities of blockchain.

These specific audiences are technical, business, and legal.

- **Technical definition**—A globally shared and secured data structure that maintains a transactional backend database that is immutable.
- **Business definition**—A business network that is used between peers to exchange value. Value can be currencies, tracking information about widgets, or anything that interested parties require to be

maintained on the blockchain ledger for any number of reasons.

- **Legal definition**—A corruption-resistant, fully auditable string of ledger entries shared over a network by multiple parties not requiring a centralized intermediary to present and validate transactions.

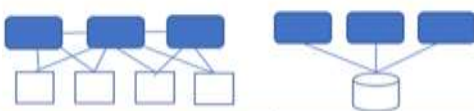
For the exam it is important to understand the definitions since this will help your greatly applying knowledge to the questions that will revolve around how value is created.

Commonly, everyone can read entries in a permissionless blockchain just by participating in the network and we know transactions cannot be deleted or modified (immutable).

Comparing Blockchain to a Database.

Figure 2.1 shows a comparison of common properties between a blockchain and a database.

Figure 2.1 - Comparison between Blockchain and a Database



Properties	Blockchain	Database
Consensus	Agreement reached by nodes	Based on database rules for commits
Operations	Create and read operations(CR)	All transactions (CRUD)
Replication	Ledger is replicated to every other blockchain node	Depends on administrative configuration
Transparency	Open to public for reads	Security controls; closed system

For example, you have a transaction pending and in the world of blockchain this transaction has to be accepted by all the other nodes in the blockchain. Blockchains work on a peer to peer protocol that require participation in typical permissionless blockchains.

The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied in blockchain. In a database this is centrally controlled and therefore could be deleted or modified by a database administrator.

Blockchain Technology

Blockchains are not built from any new transformative technology but are built from a unique syncing of three existing technologies which are peer-to-peer networks cryptography, and programs (In blockchain we refer to programs as smart contracts or dapps).

There are three primary network architectures when building an Information Technology solution.

- ✓ Centralized
- ✓ Distributed
- ✓ Decentralized.

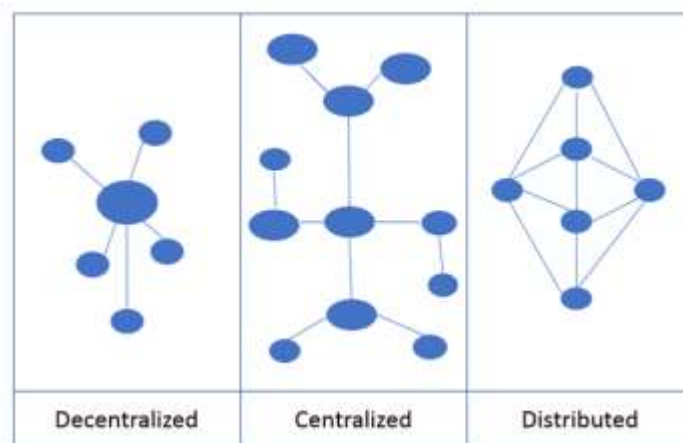
In a centralized system, both the data and the solution components are owned by a single entity, resources are concentrated in a single location or system and are easy to maintain.

In distributed systems, the data is owned by a single entity, but resources are distributed across multiple locations, data centers, and systems are not owned by the solution provider

Decentralized systems have no single owner of either data or network hardware resources as ownership and upkeep is shared amongst all participants.

Figure 2.2 shows a high-level comparison between application network architectures.

Figure 2.2 Comparing Network architectures



Another factor to consider is the cost. Even the cost of implementing these technologies is near zero when you consider there are numerous open source projects available.

Blockchains are not complex technology when viewed holistically, but the complexity can be introduced when integrating these systems into the enterprise.

Blockchains have been considered a disruptive technology since its inception which was considered as well also as the start of what has been coined the Web 3.0 generation.

Web 3.0 is the next technology front on the Web where many devices are interconnected (called the Internet of Things) and used with technologies such as automated intelligence.

Blockchains are the platform that enable our applications such as cryptocurrency and smart contracts.



Bitcoin is an unregulated digital currency that uses the blockchain technology as its transaction ledger.

What is Bitcoin?

Bitcoin is an unregulated digital currency that uses the blockchain technology as its transaction ledger.

Bitcoin was the real start of blockchain technology because it provided a use case to society for a blockchain platform in the first case.

Satoshi Nakamoto, in his 2008 paper "Bitcoin: A Peer-to-Peer Electronic Cash System," created the concept of the blockchain.

Nakamoto's paper had some detailed approaches to how a blockchain should be purposed for the masses to benefit from.

- A blockchain should be a trustless online payment network that is based on peer-to-peer (P2P) versions of electronic cash. The network is a robust node structure that works together with little coordination.
- A blockchain should alleviate the challenge of double spending, where funds can be over drafted and therefore lost to the wallet holder.
- A blockchain should implement the proof-of-work consensus method that rewards nodes that participate in the creation blocks (miners). The miners are rewarded for participation through an incentive approach, and this encourages miners to be honest.
- A blockchain should simplify privacy through a trustless system that removes intermediaries and introduces the use of anonymous public keys.

If you read Nakamoto's paper, you will likely conclude that enterprise permissioned blockchains were not in Nakamoto's vision at the time.

The realization of this requirement for enterprises was not introduced for years after Bitcoin became mainstream.



Exam will test your knowledge about Bitcoin history.

History of Blockchains

The blockchain industry really started after Nakamoto came out with Bitcoin in 2009.

However, the enterprise environment did not really get started until 2015 with permissioned blockchains. (Permissioned blockchains are generally referred to as enterprise blockchains.)

So, the blockchain technology has only been around 10 years at the time of this writing. If we consider enterprise blockchains such as Hyperledger then we are considering less than 5 years old.

Table 2.1 shows the release dates for popular blockchains into production.

Table 2.1 Blockchain Release Dates

Date	Blockchain
2009	Bitcoin
2015	Ethereum
2016	Hyperledger
2017	R3 Corda

Note that we likely know from earlier on in the chapter that Satoshi released his whitepaper in 2008.

Bitcoin whitepaper was released when? When was the Bitcoin blockchain released?

On the exam we need to learn some dates to prepare for any questions that ask about Ethereum or Bitcoin releases.



Blockchain is the enabler and cryptos are the apps that are enabled.

Comparing Blockchain to Bitcoin

Let's compare Bitcoin to a blockchain and understand how these terms come together.

Bitcoin is an unregulated digital currency that uses the blockchain technology as its transaction ledger.

A blockchain is the platform for most cryptocurrencies and is the "enabler" for Bitcoin; Bitcoin is the application (cryptocurrency) that is being "enabled."

Think of it like the blockchain is the train track, and Bitcoin is the train. Or, the blockchain is the telephone network, and Bitcoin is the phone.

Figure 1 provides a summary of comparing blockchain vs cryptos where the platform is the blockchain and Bitcoin is the application enabled by the blockchain.

Figure 2.3 provides a visual of blockchain as compared to a crypto currency.

Figure 2.3 Summary of blockchain vs cryptos



What is a difference in simple terms?



Blockchain is the train track.
(Platforms are the enabler)



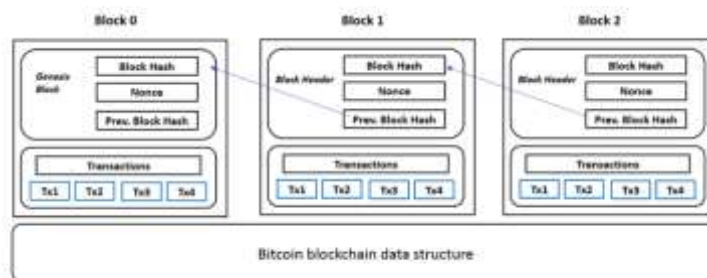
Cryptos are the train on the track.
(Applications are enabled)

At a high level, Bitcoin transactions work as follows. A sender wants to transfer funds to a recipient. The transaction is represented online as a block.

The block is broadcasted to every blockchain network participant (node). The blockchain network participants review the block, and if approved, it is added to the blockchain.

Figure 2.4 provides insight into how the Bitcoin blockchain transactions works with the previous block hashes in its data structure.

Figure 2.4 Bitcoin Blockchain Data Structure



Finally, the money moves from the sender to the recipient. Over the network (blockchain).

We will review blockchain transactions in much more detail in the upcoming chapters that cover exam objectives.



Smart Contracts
and Dapps

Smart Contracts and Dapps

Smart contracts are contracts that can be converted to code, stored, and reproduced on the network nodes. With smart contracts, you can exchange money, shares, property, and anything that is valued in a transparent manner without the services of an intermediary.

For example, through the use of an Ethereum smart contract, you could provide payment for products and have an immutable record of the transactions.

Smart contracts define the penalties and rules surrounding an agreement just like traditional contracts would when properly designed.

When you deploy several smart contracts together as an application, it is known as a *distributed application* (a *dapp* in Ethereum).

Smart contracts in Ethereum provide some significant benefits to the users of the platform, including the following:

- ✓ Autonomy
- ✓ Trust
- ✓ Backup
- ✓ Safety
- ✓ Speed
- ✓ Savings
- ✓ Accuracy

Figure 2.5 shows the workflow of an Ethereum transaction. There are four main steps to a transaction in

Ethereum, and each step must be executed properly for the next step to continue.

Settlement of the transaction can occur only if the execution of the smart contracts occurs as programmed.

Figure 2.5 Smart Contract Workflow



Settlement of the transaction can occur only if the execution of the smart contracts occurs as programmed.

Dapps are distributed applications.



Blockchain Terms
are heavily tested
on the exam.

Chapter 1 Terminology to Know for the exam.

The exam will test your knowledge around basic blockchain terminology. The below list summarizes terms briefly that commonly would likely be tested on the exam.

- ✓ A *ledger* is essentially a written or computerized record of all the transactions a business has completed.

- ✓ A *distributed ledger* is a database that is consensually shared and synchronized across networks that are spread across multiple sites, institutions, or geographies.
- ✓ Bitcoin is an unregulated digital currency that uses the blockchain technology as its transaction ledger.
- ✓ Blockchains are a globally shared data structure, with a transactional backend database that is cryptographically secure.
- ✓ Consensus is a dynamic way of reaching agreement in a group.
- ✓ Cryptocurrency is an internet-based medium of exchange that uses cryptographical functions to facilitate financial transactions in a blockchain network.
- ✓ Cryptography is the science of coding and decoding messages so as to keep messages/transactions secure.
- ✓ Dapps are distributed applications for blockchain networks that are comprised of one or more smart contracts.
- ✓ Smart Contracts are contracts that can be converted to code, stored, and reproduced on the network nodes

Practice Questions

Chapter 1

BEFORE YOU BEGIN

The main objective of these practice questions is to validate you have learned the objectives of this chapter.

1. The main benefits of Continuous Integration is really focused on specific benefits. What are two of the main benefits of a deploying a CI Pipeline?
Select Two

- A. Cost efficiency
- B. Removal of manual processes
- C. Increased revenue
- D. Removal or Risk

2. What is the