**Chapter 1**

**INTRODUCTION**

* 1. **What Is Bitcoin?**
* Unlike traditional currencies, bitcoin are entirely virtual. There are no physical coins or even digital coins per se. The coins are implied in transactions that transfer value from sender to recipient. Users of bitcoin own keys that allow them to prove ownership of bitcoin in the bitcoin network. With these keys they can sign transactions to unlock the value and spend it by transferring it to a new owner. Keys are often stored in a digital wallet on each user’s computer or smartphone. Possession of the key that can sign a transaction is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.
* Bitcoin are created through a process called “mining,” which involves competing to find solutions to a mathematical problem while processing bitcoin transactions. Any participant in the bitcoin network (i.e., anyone using a device running the full bitcoin protocol stack) may operate as a miner, using their computers processing power to verify and record transactions. Every 10 minutes, on average, a bitcoin miner is able to validate the transactions of the past 10 minutes and is rewarded with brand new bitcoin.
* The bitcoin protocol includes built-in algorithms that regulate the mining function across the network. The difficulty of the processing task that miners must perform is adjusted dynamically so that, on average, someone succeeds every 10 minutes regardless of how many miners (and how much processing) are competing at any moment.
* The protocol also halves the rate at which new bitcoin are created every 4 years, and limits the total number of bitcoin that will be created to a fixed total just below 21 million coins.
* Bitcoin represents the culmination of decades of research in cryptography and distributed systems and includes four key innovations brought together in a unique and powerful combination. Bitcoin consists of:
  + A decentralized peer-to-peer network (the bitcoin protocol)
  + A public transaction ledger (the blockchain)
  + A set of rules for independent transaction validation and currency issuance (consensus rules)
  + A mechanism for reaching global
  1. **History of Bitcoin**

Satoshi Nakamoto combined several prior inventions such as b-money and HashCash to create a completely decentralized electronic cash system.

The key innovation was to use a distributed computation system (called a “Proof-of-Work” algorithm) to conduct a global “election” every 10 minutes, allowing the decentralized network to arrive at *consensus* about the state of transactions. This elegantly solves the issue of double-spend where a single currency unit can be spent twice. Previously, the double-spend problem was a weakness of digital currency and was addressed by clearing all transactions through a central clearinghouse.

The bitcoin network started in 2009, based on a reference implementation published by Nakamoto and since revised by many other programmers.

* 1. **Getting Started**

A “bitcoin wallet” is the most common user interface to the bitcoin system. There are many implementations and brands of bitcoin wallets. bitcoin wallets vary in quality, performance, security, privacy, and reliability. There is also a reference implementation of the bitcoin protocol that includes a wallet, known as the “Satoshi Client” or “Bitcoin Core” which is derived from the original implementation written by Satoshi Nakamoto.

**1.3.1) Choosing a Bitcoin Wallet**

* Choosing a wallet is highly subjective and depends on the use and user expertise. It is therefore impossible to recommend a specific brand or project of wallet.
* Bitcoin wallets can be categorized as follows, according to the platform:

1. *Desktop wallet*

Running on general-use operating systems such as Windows and Mac OS has certain security disadvantages however, as these platforms are often insecure and poorly configured.

1. *Mobile wallet*
2. *Web wallet*

Web wallets are accessed through a web browser and store the user’s wallet on a server owned by a third party.

1. *Hardware wallet*

Hardware wallets are devices that operate a secure self-contained bitcoin wallet on special-purpose hardware. They are operated via USB with a desktop web browser or via near-field-communication (NFC) on a mobile device. By handling all bitcoin-related operations on the specialized hardware, these wallets are considered very secure and suitable for storing large amounts of bitcoin.

1. *Paper wallet*

The keys controlling bitcoin can also be printed for long-term storage. These are known as paper wallets even though other materials (wood, metal, etc.) can be used. Paper wallets offer a low-tech but highly secure means of storing bitcoin long term. Offline storage is also often referred to as *cold storage*.

* Another way to categorize bitcoin wallets is by their degree of autonomy and how they interact with the bitcoin network:

1. *Full-node client*

A full client, or “full node” is a client that stores the entire history of bitcoin transactions (every transaction by every user, ever), manages user’s wallets, and can initiate transactions directly on the bitcoin network.

A full-node client consumes substantial computer resources (e.g., more than 125 GB of disk, 2 GB of RAM) but offers complete autonomy and independent transaction verification.

1. *Lightweight client*

A lightweight client, also known as a simple-payment-verification (SPV) client, connects to bitcoin full nodes (mentioned previously) for access to the bitcoin transaction information, but stores the user wallet locally and independently creates, validates, and transmits transactions. Lightweight clients interact directly with the bitcoin network, without an intermediary.

1. *Third-party API client*

A third-party API client is one that interacts with bitcoin through a third-party system of application programming interfaces (APIs), rather than by connecting to the bitcoin network directly.

* The lines between different categories are often blurry, as many wallets run on multiple platforms and can interact with the network in different ways.
  1. **Quick Start**
* Alice downloads “Mycelium” for Android and installs it on her phone.
* When Alice runs Mycelium for the first time, as with many bitcoin wallets, the application automatically creates a new wallet for her.
* Alice is now ready to receive funds. Her wallet application randomly generated a private key.
* At this point, her bitcoin address is not known to the bitcoin network or “registered” with any part of the bitcoin system.
* It was generated independently by her wallet without reference or registration with any service. In fact, in most wallets, there is no association between the bitcoin address and any externally identifiable information including the users identity. Until the moment this address is referenced as the recipient of value in a transaction posted on the bitcoin ledger, the bitcoin address is simply part of the vast number of possible addresses that are valid in bitcoin. Only once it has been associated with a transaction does it become part of the known addresses in the network.
* Bitcoin addresses start with a 1 or 3.
* There is nothing sensitive, from a security perspective, about the bitcoin address. It can be posted anywhere without risking the security of the account.
* You can create new addresses as often as you like, all of which will direct funds to your wallet. In fact, many modern wallets automatically create a new address for every transaction to maximize privacy.
* In order to exchange bitcoin for your national currency, you will often be required to provide proof of identity and banking information. Users should be aware that once a bitcoin address is attached to an identity, all associated bitcoin transactions are also easy to identify and track. This is one reason many users choose to maintain dedicated exchange accounts unlinked to their wallets.
  1. **Finding the Current Price of Bitcoin**
* “Who sets the bitcoin price?” The short answer is that the price is set by markets.
* Bitcoin, like most other currencies, has a *floating exchange rate*. That means that the value of bitcoin vis-a-vis any other currency fluctuates according to supply and demand in the various markets where it is traded. For example, the “price” of bitcoin in US dollars is calculated in each market based on the most recent trade of bitcoin and US dollars.
  1. **Sending and Receiving Bitcoin**
* Alice has decided to exchange $10 US dollars for bitcoin. She gives Joe $10 in cash, opens her Mycelium wallet application, and selects Receive. Joe presses send to transmit the transaction. Joe’s mobile bitcoin wallet constructs a transaction that assigns 0.10 BTC to the address provided by
* Alice, sourcing the funds from Joe’s wallet and signing the transaction with Joe’s private keys. This tells the bitcoin network that Joe has authorized a transfer of value to
* Alice’s new address. As the transaction is transmitted via the peer-to-peer protocol, it quickly propagates across the bitcoin network. In less than a second, most of the well-connected nodes in the network receive the transaction and see Alice’s address for the first time.
* Meanwhile, Alice’s wallet is constantly “listening” to published transactions on the bitcoin network, looking for any that match the addresses in her wallets. A few seconds after Joe’s wallet transmits the transaction, Alice’s wallet will indicate that it is receiving 0.10 BTC.
* At first, Alice’s address will show the transaction from Joe as “Unconfirmed”. This means that the transaction has been propagated to the network but has not yet been recorded in the bitcoin transaction ledger, known as the blockchain. To be confirmed, a transaction must be included in a block and added to the blockchain, which happens every 10 minutes, on average. In traditional financial terms this is known as *clearing*.