MODULE 1

Introduction to Block chain

Blockchain is the new wave of disruption that has already started to redesign business, social and political interactions, and any other way of value exchange. Again, it is not just a change, but a rapid phenomenon that is already in motion. More than 40 top financial institutions and many different firms across industries have started to explore blockchain to lower transaction cost, speed up transaction time, reduce the risk of fraud, and eliminate the middleman or intermediary services.

Let us take a closer look at the banking system and its evolution. Starting from the olden days of barter system till fiat currencies, there was no real difference between a transaction and its settlement because they were not two separate entities. As an example, if Alice had to pay $10 to Bob, she would just hand over a $10 note to Bob and the transaction would just get settled there. No bank was needed to debit $10 from Alice's account and credit the same to Bob's account or to serve as a system of trust to ensure Alice does not cheat Bob. However, transacting directly with someone who is physically not present close by was difficult. So, banking systems evolved with many more service offerings and enabled transactions from every corner of the world. With the help of the Internet, geography was no more a limitation and banking became easier than ever. Not just banking for that matter: the Internet facilitated many different kinds of value exchange over the web. Technology enabled someone from India to make a monetary transaction with someone in the United Kingdom, but with some cost. It takes days to settle such transactions and is expensive as well. A bank was always needed to impose trust and ensure security for such transactions between two or more parties. What if technology could enable trust and security without these intermediary and centralized systems? Somehow, this part (of technology imposing trust) was missing all through, which resulted in development of centralized systems such as banks, escrow services, clearing houses, registrars and many other such institutions. Blockchain proves to be that missing piece of the Internet revolution puzzle that facilitates a trust less system in a cryptographically secured way.

Banks formed the centralized institutions that maintained the transaction records, governed interactions, enforced trust and security, and regulated the whole system. The whole of commerce relies on these financial institutions, which serve as the trusted third parties to process payments. The mediation of financial institutions increases cost and time to settle a transaction, and also limits the transaction sizes. The mediation was needed to settle disputes, but that meant that completely non-reversible transaction was never possible. This resulted in a situation where trust was needed for someone to transact with another. Certainly, this bureaucratic system had to change to keep up with the economy's expected digital transformation. So, a cryptocurrency called Bitcoin was invented which was enabled by the underlying technology— blockchain. Bitcoin is just one monetary use case of blockchain that addresses the inherent weakness of trust-based models.

What is Blockchain?

The Internet has revolutionized many aspects of life, society, and business. However, the way people and organizations execute transactions with one another has not changed much in the past couple of decades. Blockchain is believed to be the component that completes the Internet puzzle and makes it more open, more accessible, and more reliable. To understand blockchain, you have to understand it from both a **business perspective** and **technical perspective**. Let us first

understand it in a business transaction context to get the **"what"** of it, and then look into the technicality to understand the **"how"** of it.

Blockchain is a system of records to transact value (not just money!) in a peer-to-peer fashion. What it means is that there is no need for a trusted intermediary such as banks, brokers, or other escrow services to serve as a trusted third party. For example, if Alice pays to Bob $10, why would it go through a bank? Take a look at the Figure 1-1.

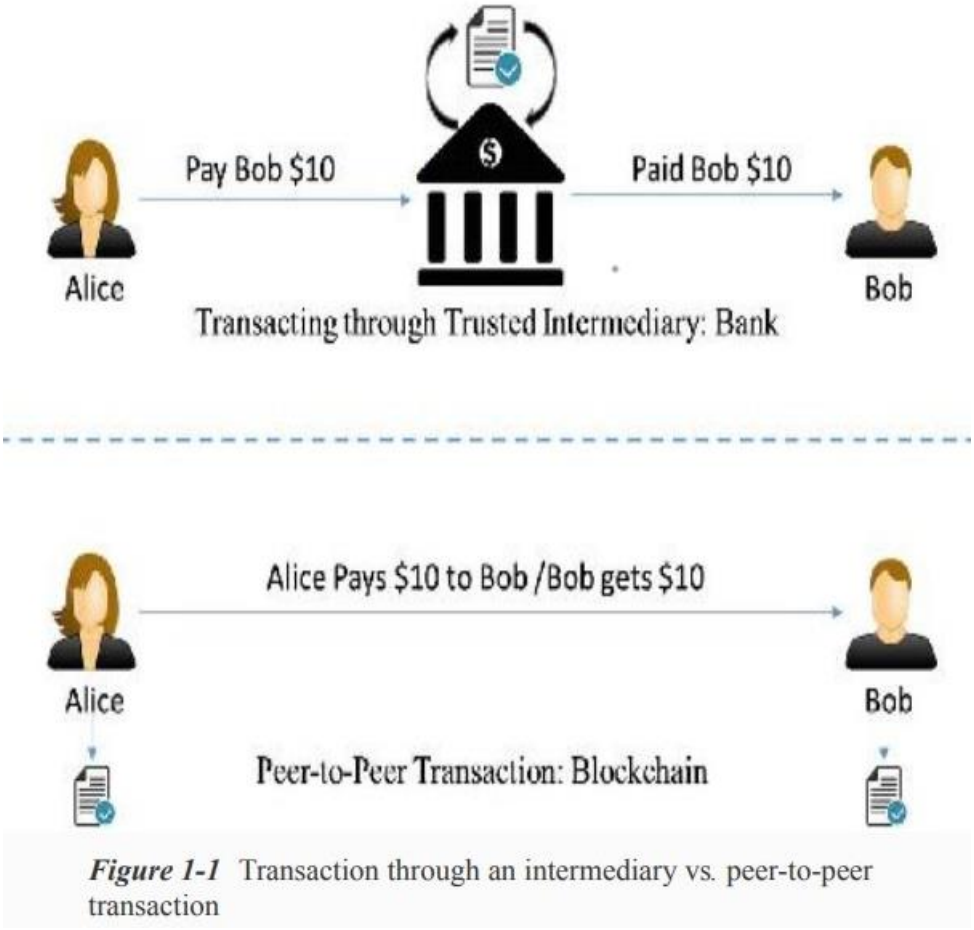


Figure 1-1 Transaction through an intermediary vs. peer-to-peer transaction

Let us look at a different example now. A typical stock transaction happens in seconds, but its settlement takes weeks. Is it desirable in this digital age? Certainly not!

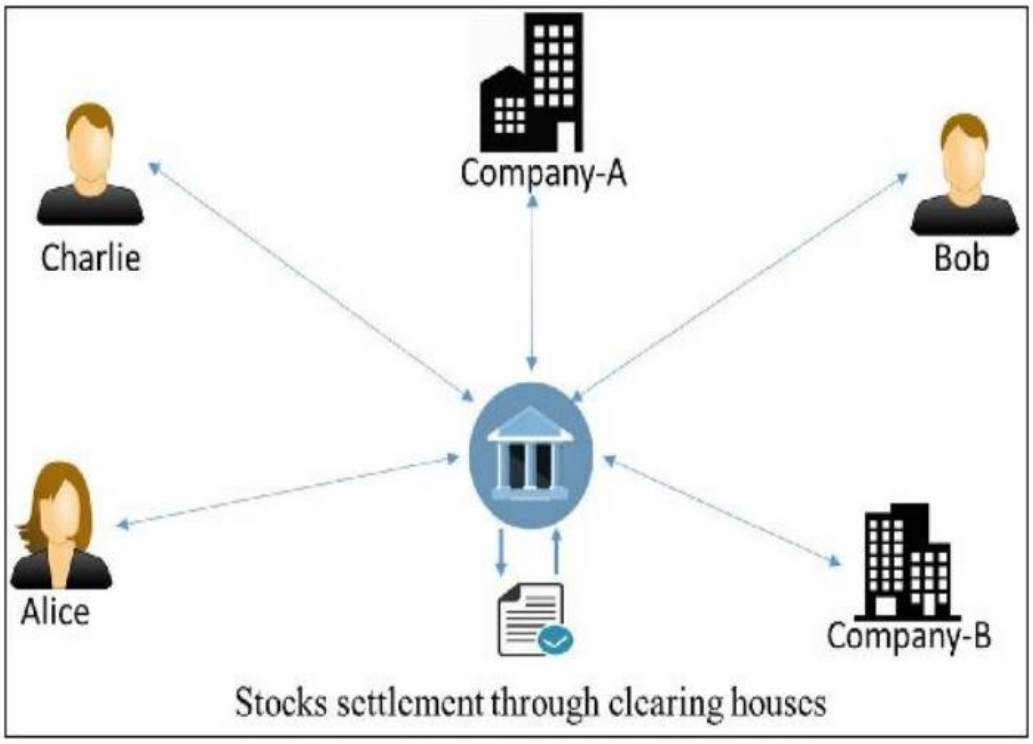


Figure 1-2 Stocks trading through an intermediary clearing house

If someone wants to buy some stocks from a company or a person, they can just directly buy it from them with instant settlement, with no need for brokers, clearing houses, or other financial institutions in between. A decentralized and peer-to-peer solution to such a situation can be represented as in Figure 1-3.

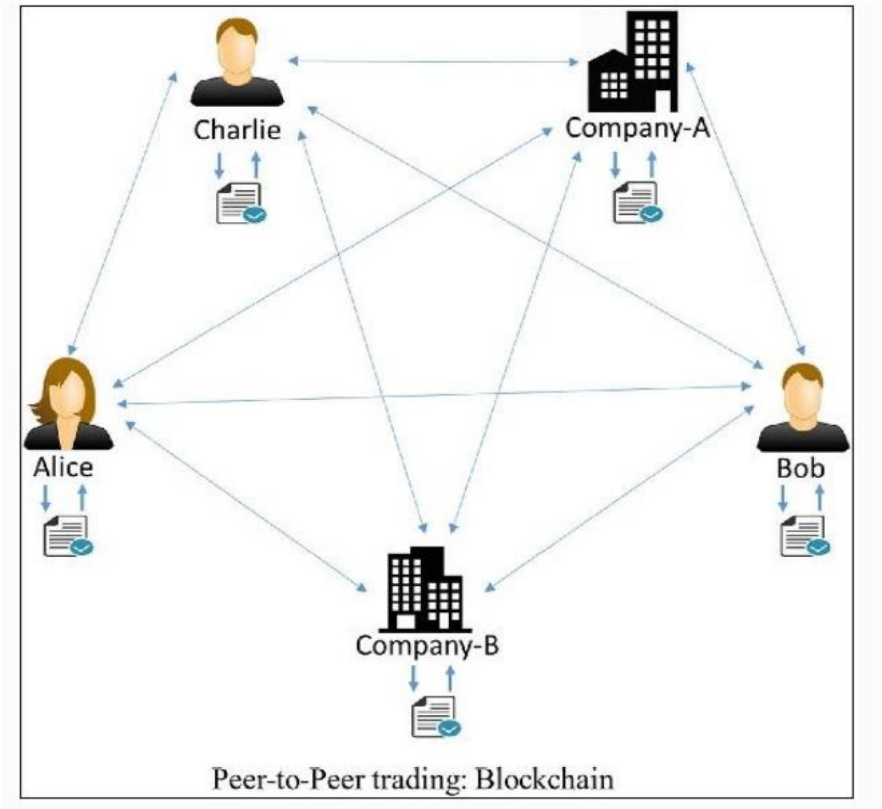


Figure 1-3 Peer-to-peer stock trading

Transaction and settlement are not two different entities in a blockchain setting. The transactions are analogous to, say, fiat currency transactions where if someone pays another a $10 note, they do not own it anymore and that $10 note is physically transferred to the new owner.

Salient Features:

- Blockchain is a peer-to-peer system of transacting values with no trusted third parties in between.
- It is a shared, decentralized, and open ledger of transactions. This ledger database is replicated across a large number of nodes.
- This ledger database is an append-only database and cannot be changed or altered. It means that every entry is a permanent entry. Any new entry on it gets reflected on all copies of the databases hosted on different nodes.
- There is no need for trusted third parties to serve as intermediaries to verify, secure, and settle the transactions.
- It is another layer on top of the Internet and can coexist with other Internet technologies.
- Just the way TCP/IP was designed to achieve an open system, blockchain technology was designed to enable true decentralization. In an effort to do so, the creators of Bitcoin open-sourced it so it could inspire many decentralized applications.

A typical blockchain may look as shown in Figure 1-4.

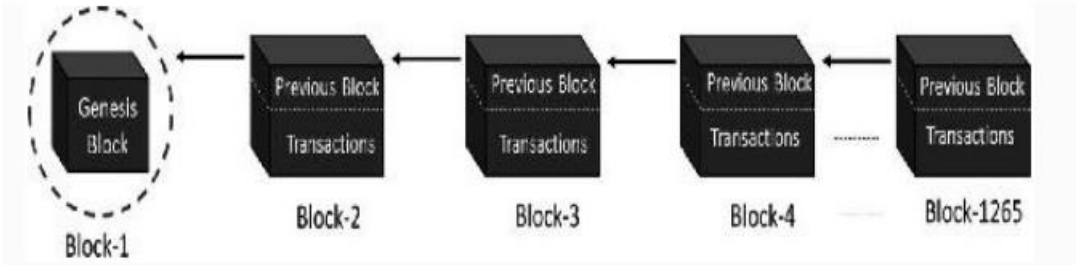


Figure 1-4 The blockchain data structure

Every node on the blockchain network has an identical copy of the blockchain shown in Figure 1-4, where every block is a collection of transactions, hence the name. As you can see, there are two major parts in every block. The “header” part links back to the previous block in the chain. What it means is that every block header contains the hash of the previous block so that no one can alter any transaction in the previous block. The other part of a block is the “body content” that has a validated list of transactions, their amounts, the addresses of the parties involved, and some more details. So, given the latest block, it is feasible to access all the previous blocks in a blockchain.

How Blockchain works?

Let us consider a practical example and see how the transactions take place and the ledger gets updated across the network, to see how this system works: Assume that there are three candidates—Alice, Bob, and Charlie—who are doing some monetary transactions among each other on a blockchain network. Let us go through the transactions step by step to understand blockchain’s open and decentralized features.

Step-1:

Let us assume that Alice had $50 with her, which is the genesis of all transactions and every node is aware of it, as shown in Figure 1-5.

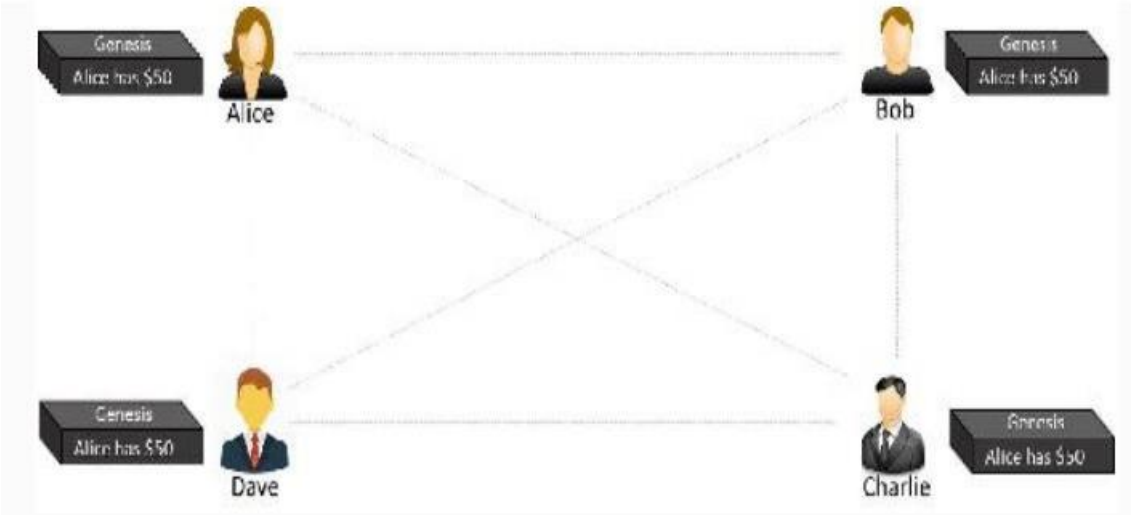


Figure 1-5 The genesis block

Step-2: Alice makes a transaction by paying $20 to Bob. Observe how the blockchain gets updated at each node, as shown in Figure 1-6.

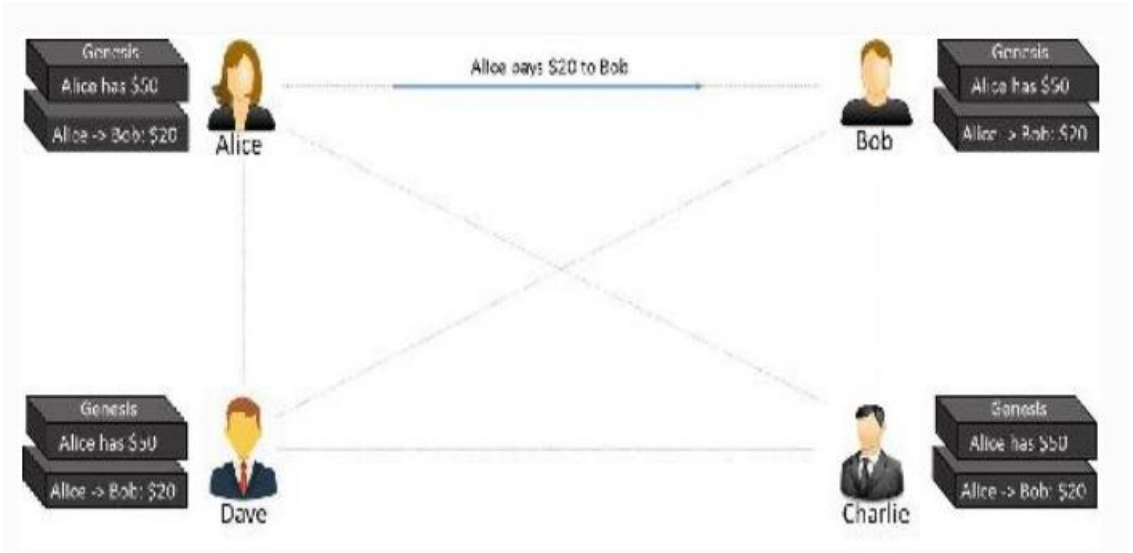


Figure 1-6 The first transaction

Step-3: Bob makes another transaction by paying $10 to Charlie and the blockchain gets updated as shown in Figure 1-7.

Figure 1-7 The second transaction

Note that the transaction data in the blocks is immutable. All transactions are fully irreversible. Any change would result in a new transaction, which would get validated by all contributing nodes. Every node has its own copy of blockchain.

If there are many questions popping up in your mind, such as "What if Alice pays the same amount to Dave to double-spend the same amount, or what if she is making a payment without having enough funds in her account?" "How is the security ensured?" and so on, we are going to cover those details in the following chapters.

Centralized Vs. Decentralized Systems

The very reason we are looking into the debate on centralization vs. decentralization is because blockchain is designed to be decentralized, defying the centralized design. Note that whether a system is centralized or decentralized, it can still be distributed. A centralized distributed system is one in which there is, say, a master node responsible for breaking down the tasks or data and distribute the load across nodes. On the other hand, a decentralized distributed system is one where there is no "master" node as such and yet the computation may be distributed. Blockchain is one such example. Figure 1-8 is a pictorial representation of how a centralized distributed system may look.

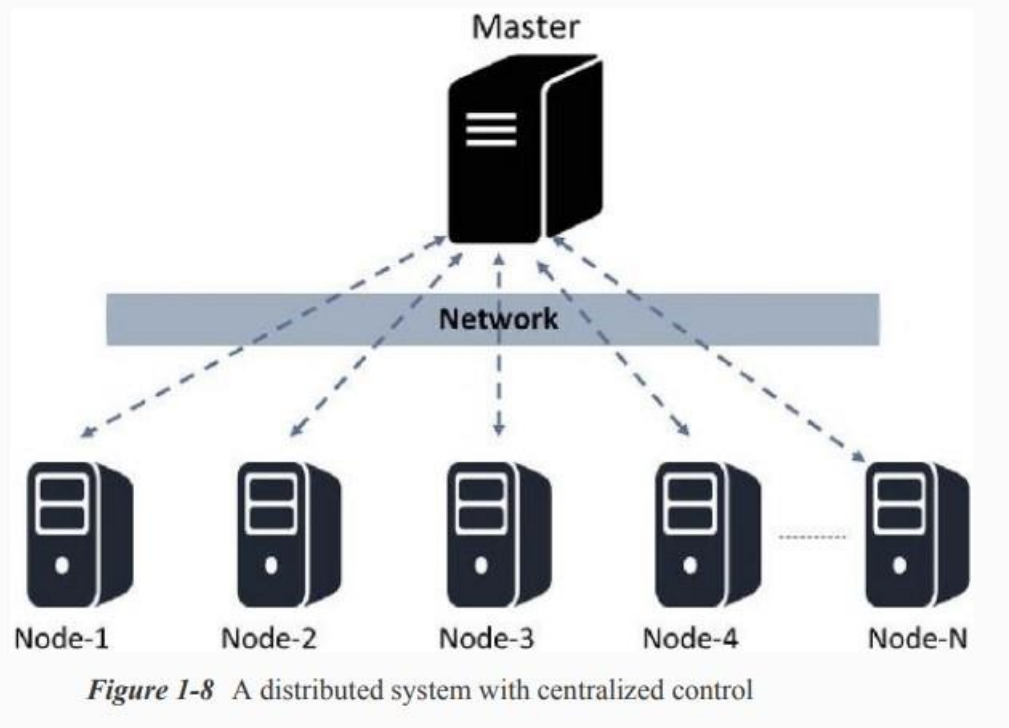


Figure 1-8 A distributed system with centralized control

Though the computation is faster in such designs because of distributed computing, it also suffers from limitations due to centralization.

Layers of Blockchain

The public blockchain variants such as Ethereum are in the process of maturing, and building complex applications on top of these blockchains may not be a good idea. Keep in mind that blockchain is never just a piece of technology, but a combination of business principles, economics, game theory, cryptography, and computer science engineering. Most of the real-world applications are quite complex in nature, and it is advisable to build blockchain solutions from the ground up. To start with, let us just recollect our basic understanding of the TCP/IP protocol stack. The layered approach in the TCP/IP stack is actually a standard to achieve an open system. Having abstraction layers not only helps in understanding the stack better, but also helps in building products that are compliant to the stack to achieve an open system. Also, having the layers abstract from each other makes the system more robust and easy to maintain. Any change to any of the layers doesn't impact the other layers. Again, the TCP/IP analogy is not to be confused with the blockchain layers. TCP/IP is a communication protocol that every Internet application uses, and so is blockchain. There are no agreed global standards yet that would clearly segregate the blockchain components into distinct layers. A layered heterogeneous architecture is needed, but for now that is still in the future. So, we will try to formulate blockchain layers to be able to understand the technology better and build a comparative analogy between hundreds of blockchain/Cryptocurrency variants out there in the market. Take a look at the high-level, layered representation of blockchain in Figure 1-12.

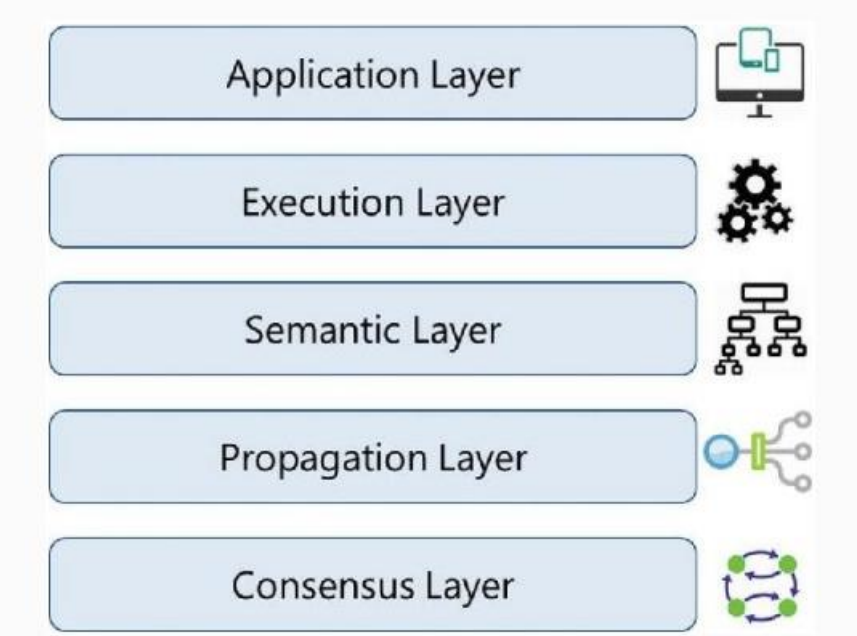


Figure 1-12 Various layers of blockchain

There cannot be too many or too few layers; it is going to be a trade-off driven among complexity, robustness, adaptability, etc., to name a few. The purpose again is not really to standardize blockchain technology, but to build a better understanding. Note that all these layers are present on all the nodes.

In later modules, we will be building a decentralized application from scratch and learning how blockchain functions on all these layers with a practical use case.

i. Application Layer

Because of the characteristics of blockchain, such as immutability of data, transparency among participants, resilience against adversarial attacks etc., there are multiple applications being built. Certain applications are just built in the application layer, taking for granted any available "flavor" of blockchain, and some applications are built in the application layer and are interwoven with other layers in blockchain. This is the reason the application layer should be considered a part of blockchain. This is the layer where you code up the desired functionalities and make an application out of it for the end users. For the applications that treat blockchain as a backend, those applications might need to be hosted on some web servers. Ideally, good blockchain applications do not have a client–server model, and there are no centralized servers that the clients access, which is just the way Bitcoin works. You probably have heard or already learned about the off-chain networks. The idea is to build applications that wouldn't use blockchain for anything and everything, but use it wisely. In other words, this concept is to ensure that the heavy lifting is done at the application layer, or bulky storage requirements are taken care of off the chain so that the core blockchain is light and effective and the network traffic is not too much.

ii. Execution Layer

The Execution Layer is where the executions of instructions ordered by the Application Layer take place on all the nodes in a blockchain network. The instructions could be simple instructions or a set of multiple instructions in the form of a smart contract. In either case, a program or a script needs to be executed to ensure the correct execution of the transaction. All the nodes in a blockchain network have to execute the programs/scripts independently. Deterministic execution

of programs/scripts on the same set of inputs and conditions always produces the same output on all the nodes, which helps avoid inconsistencies. In the case of Bitcoins, these are simple scripts that are not Turing-complete and allow only a few set of instructions. Ethereum and Hyperledger, on the other hand, allow complex executions. Ethereum's code or its smart contracts written in solidity gets compiled to Bytecode or Machine Code that gets executed on its own Ethereum Virtual Machine. Hyperledger has a much simpler approach for its chaincode smart contracts. It supports running of compiled machine codes inside docker images, and supports multiple high-level languages such as Java.

iii. Semantic Layer

The Semantic Layer is a logical layer because there is an orderliness in the transactions and blocks. A transaction, whether valid or invalid, has a set of instructions that gets through the Execution Layer but gets validated in the Semantic Layer. If it is Bitcoin, then whether one is spending a legitimate transaction, whether it is a double-spend attack, whether one is authorized to make this transaction, etc., are validated in this layer. It is the semantic layer that defines how the blocks are linked with each other. Every block in a blockchain contains the hash of the previous block, all the way to the genesis block. Though the final state of the blockchain is achieved by the contributions from all the layers, the linking of blocks with each other needs to be defined in this layer. Depending on the use case, you might want to code up an additional functionality in this layer.

iv. Propagation Layer

The previous layers were more of an individual phenomenon: not much coordination with other nodes in the system. The Propagation Layer is the peer-to-peer communication layer that allows the nodes to discover each other, and talk and sync with each other with respect to the current state of the network. When a transaction is made, we know that it gets broadcast to the entire network. Similarly, when a node wants to propose a valid block, it gets immediately propagated to the entire network so that other nodes could build on it, considering it as the latest block. So, transaction/block propagation in the network is defined in this layer, which ensures stability of the whole network. By design, most of the blockchains are designed such that they forward a transaction/block immediately to all the nodes they are directly connected to, when they get to know of a new transaction/block. In the asynchronous Internet network, there are often latency issues for transaction or block propagation. Some propagations occur within seconds and some take more time, depending on the capacity of the nodes, network bandwidth, and a few more factors.

v. Consensus Layer

The Consensus Layer is usually the base layer for most of the blockchain systems. The primary purpose of this layer is to get all the nodes to agree on one consistent state of the ledger. There could be different ways of achieving consensus among the nodes, depending on the use case. Safety and security of the blockchain is ascertained in this layer. In Bitcoin or Ethereum, the consensus is achieved through proper incentive techniques called "mining." For a public blockchain to be self-sustainable, there has to be some sort of incentivization mechanisms that not only helps in keeping the network alive, but also enforces consensus. Bitcoin and Ethereum use a Proof of Work (PoW) consensus mechanism to randomly select a node that can propose a block. Once that block is proposed and propagated to all the nodes, they check to see if it a valid block with all legitimate transactions and that the PoW puzzle was solved properly; they add this block to their own copy of blockchain and build further on it. There are many different variants of

consensus protocols such as Proof of Stake (PoS), deligated PoS (dPoS), Practical Byzantine Fault Tolerance (PBFT), etc.

Blockchain Vs. Bitcoin

i. Blockchain

In Blockchain every block contains a cryptographic hash of the previous block, a timestamp, and transaction information. In other words, blockchain is a distributed database technology, which restricts bitcoin or any digital asset. It enables multiple parties to transact, share valuable data, and pool their resources in a secure yet tamper-proof manner. Data contained within the blockchain is distributed across many computers and is therefore decentralized. Due to decentralized nature, blockchains are incredibly secure as there is no single point of attack.

ii. Bitcoin

The Bitcoin Network is the network of computers throughout the world that are connected together, to actually process Bitcoin payment transactions between Bitcoin accounts. These computers are referred to as miners and are owned by individual people and companies around the world. The Bitcoin Network is very secure. There is no possibility of 'Double Spending' and the system has been specifically designed and coded to make creating counterfeit Bitcoin or fake transactions impossible. Bitcoin is one of the earliest cryptocurrencies to use blockchain technology in facilitating peer-to-peer payments. Through a decentralized network, bitcoin offers a reasonably low transaction fee compared to popular payment gateways.

S.No.	Basis of Comparison	Blockchain	Bitcoin
1.	What is it?	A Distributed Database	A cryptocurrency
2.	Main Aim	To provide a low cost, safe and secure environment for peer to peer transactions	To simplify and increase the speed of transactions without much of government restrictions.
3.	Trade	Blockchain can easily transfer anything from currencies to property rights of the stock	Bitcoin is limited to trading as a currency.
4.	Scope	It is more open to changes and hence has the backing of many top companies.	The scope of bitcoin is limited.

S.No.	Basis of Comparison	Blockchain	Bitcoin
5.	Strategy	Blockchain can be adapted to any changes and hence it can cater to different industries.	Bitcoin focuses on lowering the cost of influencers and reducing the time of transactions but is less flexible.
6.	Status	As blockchain works with various businesses, it should have compliance with KYC and other norms. Hence blockchain is transparent.	Bitcoin likes to be anonymous and hence even though we can see the transactions in the ledger, they are numbers that are not in a particular sequence.

- **Key Differences**

To finish up, let's recap why blockchain and Bitcoin are two completely separate things:

- Bitcoin is a cryptocurrency, while blockchain is a distributed database.
- Bitcoin is powered by blockchain technology, but blockchain has found many uses beyond Bitcoin.
- Bitcoin promotes anonymity, while blockchain is about transparency. To be applied in certain sectors (particularly banking), blockchain has to meet strict Know Your Customer rules.
- Bitcoin transfers currency between users, while blockchain can be used to transfer all sorts of things, including information or property ownership rights.

Practical Applications

In this section, we will look at some of the initiatives that are already being taken across industries such as finance, insurance, banking, healthcare, government, supply chains, IoT (Internet of Things), media and entertainment to name a few. The possibilities are limitless. A true sharing economy, which was difficult to achieve in centralized systems, is possible using blockchain technology (e.g., peer-to-peer versions of Uber, AirBNB). It is also possible to enable citizens to own their identity (Self-Sovereign Digital Identity) and monetize their own data using this technology. For now, let us take a look at some of the existing use cases.

- Any type of property or asset, whether physical or digital, such as laptops, mobile phones, diamonds, automobiles, real estate, e-registrations, digital files, etc. can be registered on blockchain. This can enable these asset transactions from one person to another, maintain the transaction log, and check validity or ownerships. Also, notary services, proof of existence, tailored insurance schemes, and many more such use cases can be developed.

- There are many financial use cases being developed on blockchain such as cross-border payments, share trading, loyalty and rewards system, Know Your Customer (KYC) among banks, etc. Initial Coin Offering (ICO) is one of the most trending use cases. ICO is the best way of crowdsourcing today by using cryptocurrency as digital assets. A coin in an ICO can be thought of as a digital stock in an enterprise, which is very easy to buy and trade.
- Blockchain can be used to enable "The Wisdom of Crowds" to take the lead and shape businesses, economies, and various other national phenomena by using collective wisdom! Financial and economic forecasts based on the wisdom of crowds, decentralized prediction markets, decentralized voting, as well as stocks trading can be possible on blockchain.
- The process of determining music royalties has always been convoluted. The Internet-enabled music streaming services facilitated higher market penetration, but made the royalty determination more complex. This concern can pretty much be addressed by blockchain by maintaining a public ledger of music rights ownership information as well as authorised distribution of media content.
- This is the IoT era, with billions of IoT devices everywhere and many more to join the pool. A whole bunch of different makes, models, and communication protocols makes it difficult to have a centralized system to control the devices and provide a common data exchange platform. This is also an area where blockchain can be used to build a decentralized peer-to-peer system for the IoT devices to communicate with each other. ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) is a joint initiative from IBM and Samsung that has developed a platform that uses elements of the Bitcoin's underlying design to build a distributed network of devices—a decentralized IOT. ADEPT uses three protocols: BitTorrent for file sharing, Ethereum for smart contracts, and TeleHash for peer-to-peer messaging in the platform. The IOTA foundation is another such initiative.
- In the government sectors as well, blockchain has gained momentum. There are use cases where technical decentralization is necessary, but politically should be governed by governments: land registration, vehicle registration and management, e-Voting, etc. are some of the active use cases. Supply chains are another area where there are some great use cases of blockchain. Supply chains have always been prone to disputes across the globe, as it was always difficult to maintain transparency in these systems.

Basics of Public and Private Keys

Public and private keys are an integral part of Bitcoin and other cryptocurrencies. They allow you to send and receive cryptocurrency without requiring a third party to verify the transactions. These keys are a part of the public-key cryptography (PKC) framework. You can use these keys to send your cryptocurrency to anyone, anywhere, at any time. The public and private keys fit together as a key pair. You may share your public keys in order to receive transactions, but your private keys must be kept secret. If anyone has access to the private keys, they will also have access to any cryptocurrency associated with those keys.

i. Public Key Cryptography (PKC)

Public-key cryptography (PKC) is a technology often used to validate the authenticity of data using asymmetric encryption. PKC was first used primarily to encrypt and decrypt messages in traditional computing. Cryptocurrencies now use this technology to encrypt and decrypt transactions. Without PKC, the technology underpinning cryptocurrencies would be practically impossible.

The key to PKC is “trapdoor functions,” one-way mathematical functions that are easy to solve in one way, but nearly impossible to crack in the reverse. While it might be possible, it would likely take a supercomputer — and thousands of years — to reverse engineer these functions.

ii. Public Key

A public key allows you to receive cryptocurrency transactions. It’s a cryptographic code that’s paired to a private key. While anyone can send transactions to the public key, you need the private key to “unlock” them and prove that you are the owner of the cryptocurrency received in the transaction. The public key that can receive transactions is usually an address, which is simply a shortened form of your public key. Therefore, you can freely share your public key without worry. You may have seen donation pages for content-creators or charities with the public keys for their crypto addresses online. While anyone can donate, you’d need the private key to unlock and access the donated funds.

iii. Private Key

Here is one crucial piece of advice to remember: Never share your private key with anyone. A private key gives you the ability to prove ownership or spend the funds associated with your public address. A private key can take many forms:

- 256 character long binary code
- 64 digit hexadecimal code
- QR code
- Mnemonic phrase

Regardless of its form, a private key is an astronomically large number, and it’s large for a good reason. While you can generate a public key with a private key, doing the opposite is practically impossible because of the one-way “trapdoor” function. You can have any number of public keys connected to a private key.

iv. Digital Signing of a Transaction

For a transaction on the blockchain to be complete, it needs to be signed. The steps for someone to send you a transaction are:

- A transaction is encrypted using a public key. The transaction can only be decrypted by the accompanying private key.
- Next, the transaction is signed using the private key, which proves that the transaction hasn’t been modified. The digital signature is generated through combining the private key with the data being sent in the transaction.
- Finally, the transaction can be verified as authentic using the accompanying public key.

You digitally sign a transaction to prove you’re the owner of the funds. Nodes check and authenticate transactions automatically. Any unauthenticated transactions get rejected by the network. An authentic, mined transaction on the blockchain is irreversible.

v. Where are the “Private Keys?”

Your private keys are in a cryptocurrency wallet, which is typically mobile or desktop software or a specialized hardware device. Your private keys are not on the cryptocurrency blockchain network. If you keep cryptocurrency on an exchange, then the exchange is the custodian of your private keys; you’re trusting it with your keys in the same way you’d trust a bank’s vault to hold your gold.

If you transfer your cryptocurrency from an exchange to a non-custodial wallet, then you are in control of your keys. Because of the configuration and functionality of cryptocurrency wallets, you'll likely never handle the private keys directly as wallets generally manage them for you automatically. Typically, you're given a seed phrase that encodes your private keys as a back-up.

vi. Public and Private Keys Control Crypto

How public and private keys work together is fundamental to understanding how cryptocurrency transactions function. When you say you have cryptocurrency, what you're really saying is you have a private key that proves ownership of that cryptocurrency. Since it's stored on the blockchain, anyone can verify you as the owner with your public key.

The choice of "holding your own keys" or trusting a custodian depends on your philosophy, risk-tolerance, and a host of other factors. If you hold your own private keys, consider modern HD wallets, which can do a great job of managing your private keys, and remember to never share them. If you choose a custodial solution like an exchange, make sure you choose a trusted, reputable company that places a high emphasis on security and regulation.

Pros and Cons of Blockchain

Let's look at the most significant blockchain advantages and why businesses and individuals are eager to adopt the technology. Some disadvantages are also put forward.

Advantages:

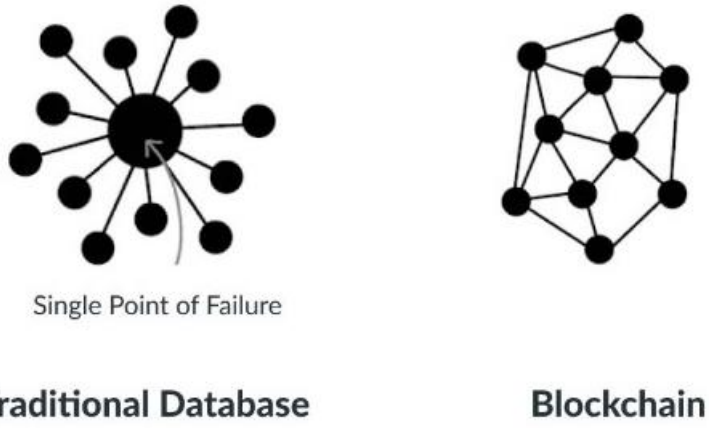
i. Decentralized Trust

One of its biggest strengths is that you no longer need to trust a third party to make any transaction. People using blockchain worldwide are confident that no single party is manipulating transactions, viewing personal information or performing any other activity breaching their privacy and security. That doesn't mean blockchain-based applications are always secure—that depends on how good developers are at creating secure code—but it does mean there are opportunities for better security than conventional applications. With blockchain, you can feel more confident about your data and identity. You only share what you want; companies cannot see your data without your permission. You can also feel more confident about getting paid for providing services. With blockchain, payment is instant; there's no need to wait days for money orders or checks to clear.

ii. Low Operational Cost

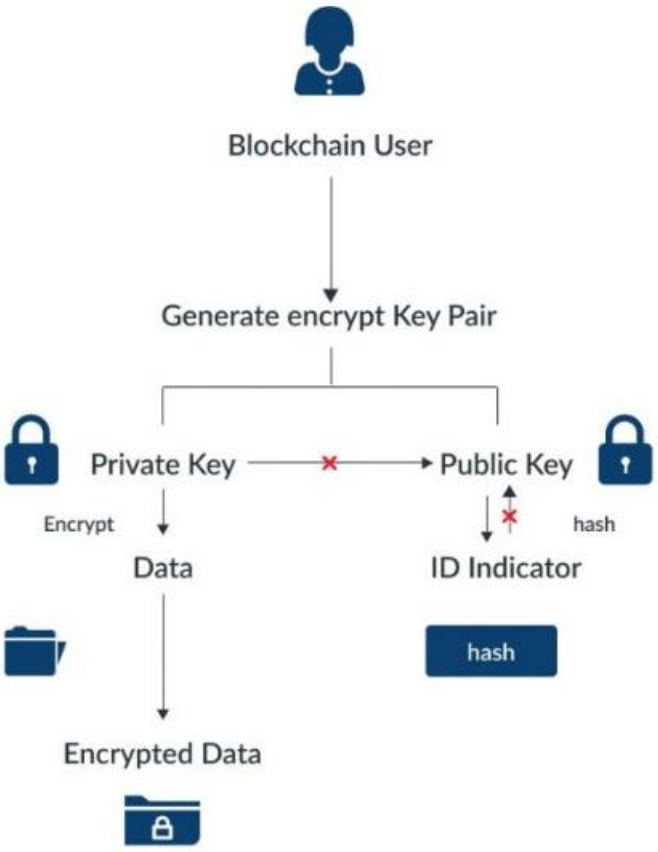
Blockchain reduces overhead costs as it has no centralized authority or servers to maintain operations. There is no payment processing or banking fees as it opts for peer-to-peer transactions without third-party approval. It embeds documents, agreements, or transactions within the system. Blockchain encryptions are more secure against identity theft than conventional payment systems.

iii. No Single Point of Failure



With blockchain technology, there's no single point of failure. If a hacker were to gain access to your business's server or database, they could very easily wipe out your entire network—all at once. Blockchain technology is not centralized; instead, it is in distributed form. It saves your data if the network goes down as hackers cannot break into the central grid and affect any connected account. You can create passwords up to 100 characters long, making it impossible for hackers to guess or decode. It gives better security than regular networks with the option of up to 8-character long passwords (including letters and numbers).

iv. Enhanced Security and Confidentiality



Being distributed across a global network of computers and protected by cryptography, blockchain technology is inherently more secure than centralized systems. It is tough to tamper with records once they are in there. Any attempt to alter one's record will reflect immediately

because copies and digital signatures are checked against each other automatically. It has an added layer of confidentiality that secures your data from hackers. Transactions are impossible to trace or link back to an individual user. The user can select their names and e-mail addresses during transactions. You get the option to complete your transactions while remaining anonymous. So, you can use blockchain-based services without worrying about advertisers tracking your activity or identity thieves accessing sensitive information such as credit card numbers.

v. Quick Transactions

Blockchain is capable of processing much faster transactions than any traditional bank. As a result, businesses that use blockchain instead of banks can save a considerable amount on fees. Deloitte has predicted that blockchain technology could save companies up to billions in the form of banking fees. Blockchain's decentralized structure doesn't require massive data centers and expensive third-party verification. It also limits the number of people involved in monitoring the transactions.

vi. Reduces Fraud

Blockchain technology has some attributes that make it ideal for financial institutions to reduce forgery. It records every activity, making it impossible for anyone to make duplicate transactions. Each block stores the financial information, and if any modification is made to a previous block, other nodes on the network reject it.

vii. Transparent and Universal Recording System

The transactions in the blockchain are recorded in a public ledger that anyone can view. All can see the amount stored in the wallet but cannot identify its owner. A wallet could be tied to an individual or group. Still, if users want to remain anonymous, they must transfer their Bitcoins to another address (e.g., a different Bitcoin wallet) that isn't linked with their real identity. But even without anonymity features enabled, blockchain tech provides more transparency than traditional payment methods like credit cards and checks; you don't need a bank intermediary (or permission from one) to see what or whom you paid or received money from.

viii. Better Accessibility

A blockchain allows anyone with a computer and an internet connection to be part of its network. It is decentralized, meaning any single entity can't control it—and everyone has equal access to it. Anyone can make changes (add information) or add new blocks (to store data) to a blockchain, provided they know how to do so. Even non-tech individuals have the same access to blockchains. This openness makes blockchains much more accessible than traditional institutions like banks and financial services. That doesn't mean you shouldn't be wary when dealing with blockchain providers: you should always research your choices before making any significant financial decisions.

ix. Prevents Double Spending

Bitcoin transactions are verified by network nodes through cryptography and recorded in a publicly distributed ledger called a blockchain. This ensures safety by eliminating direct access to your money. That's why some say bitcoin is fungible—its value is equal even if its physical form changes. In other words, bitcoins derive their worth from mathematics alone, unlike fiat currencies like U.S. dollars or euros, which get their value from an organization's financial

standing. Every single bitcoin carries all its transactional histories within that particular blockchain framework.

x. Seamless Integration into Existing Systems

Blockchain offers seamless integration of their current financial systems into the outside networks. It can be done in two ways: Blockchain as a Service (BaaS) and blockchain application platforms. BaaS offers organizations a secure connection to blockchain networks using cloud services, while blockchain application platforms allow anyone – even those without cloud services – to use blockchain technology. The integration process is much more seamless than other means of blockchain access. Blockchain as a Service allows businesses to connect directly with blockchain networks, giving them immediate access to these decentralized ledgers. It doesn't force you to use one blockchain or another and gives you a higher level of control than some other methods. Additionally, BaaS is typically quicker and easier to set up than other services, making it ideal for organizations that may need blockchains immediately, such as supply chain management applications.

Disadvantages:

- Scalability

Blockchain is capable of handling fewer transactions per second. It causes delays in finalizing the massive volume of transactions resulting in poor scalability. However, several methods have been proposed to overcome this shortcoming, but none has been implemented till now.

- Security

Blockchain is publicly accessible as a distributed ledger. It may attract any unknown visitor monitoring your wallet. Though there are several provisions to add privacy and encryption layers to enable your preferred privacy, all are not commonplace yet. Moreover, much of your data is linked directly to your digital identity, so it could potentially expose parts of your private life that you wouldn't necessarily want online. Security concerns often lead people to trust third-party solutions (like exchanges) over direct blockchain transactions, relinquishing control over personal assets.

- Cost

One of the biggest problems with blockchain technology is that it requires enormous energy. Because miners have to solve complicated math problems to get a payout, they need powerful rigs that consume tons of electricity. As a result, some blockchains are incredibly costly to run, especially for smaller businesses or individuals. You cannot make changes later; if you want your blockchain online, you must pay for it up front!

- Competitiveness

There is a lot of hype surrounding these industries trying to use blockchain. It leads to unnecessary competition between businesses as they opt for this technology and waste their time, money, and efforts even when it is useless for their business. Companies will have no alternative but to invest heavily to keep up with their competitors.

- Speed

The other significant con to blockchain technology is its speed. Unlike a centralized database, blockchains require miners—or people with high-end computers and dedicated software that solve computational puzzles in exchange for new crypto tokens. In simple terms, blockchain

transactions take longer than traditional payment methods like cash or credit cards. This can be discouraging if you're interested in using blockchain technology as a daily payment method.

Myths about Bitcoin

Myth 1: Bitcoin Is Anonymous

A common misconception of Bitcoin is that its users are anonymous. However, this is far from true. Because each bitcoin belongs to an address, all bitcoins have a clear and visible history of ownership tracing back to their creation. In addition, the Bitcoin blockchain allows all transactions to be viewed by anyone in the network, so transactions, addresses, and supply can be easily audited by any and all network participants. Addresses however, are merely strings of letters and numbers, and are not inherently connected to a given user or wallet. Both users and wallets can use an arbitrary number of addresses to store bitcoin, and some addresses, called **multisig** addresses, can hold bitcoin belonging to multiple users. Thus, Bitcoin is most accurately defined as pseudonymous rather than anonymous.

- Block explorers are a software tool that allow blockchain transaction data to be audited. They audit transactions by confirming the bitcoin quantity of a bitcoin address on a given date matches the transaction specifications.

Myth 2: Bitcoin Is Not Backed and Has No Inherent Value

While Bitcoin is not backed in the sense that it has a guaranteed rate of exchange for another asset, Bitcoin is backed in the same way that traditional fiat currencies are backed: demand and support from its users. Its value is guaranteed by its market participants and utility. Unlike fiat currencies, the long-term value of Bitcoin is assured by its limited supply. The limited supply of Bitcoin protects against inflation, which has historically crippled many fiat currencies.

Myth 3: The Bitcoin Blockchain Is Insecure

Often, the transparency of the Bitcoin blockchain is misinterpreted as a security failing. However, the public nature of the Bitcoin network allows it to remain secured by the millions of miners, traders, and investors active on the network. In order to corrupt the Bitcoin blockchain, it would be necessary to control at least 51% of all the computing power associated with the network. With millions of computers and users around the world participating in the Bitcoin network, the potential for any one entity to control a majority of the network is incredibly limited.

Myth 4: Bitcoin Is Unregulated and Unsupported by Governments

Major U.S. government figures, including the Federal Reserve, presidential candidates, senators, and state-elected officials, have acknowledged Bitcoin and supported formal regulation. In the United States, Bitcoin is regulated at both the state and federal level. Companies and individual investors that engage with Bitcoin are required to complete rigorous due diligence, comparable to the requirements of those that engage with traditional investment assets. Bitcoin exchanges and brokerages are likewise subject to the exact same regulation as most traditional brokerages and exchanges.

Myth 5: Bitcoin Is Difficult to Understand and the Barriers to Entry Are High

Bitcoin may be an intimidating concept, but the information detailing why and how Bitcoin was creating and how it operates is widely available. Satoshi Nakamoto, the creator of Bitcoin, ensured that the Bitcoin blockchain and its white paper would be publicly accessible so that anyone could participate in the Bitcoin market. In addition, opening a personal wallet for Bitcoin transactions is

fast and simple. Finally, Bitcoin is highly divisible into portions of bitcoin known as satoshis, which can be purchased for fractions of a cent.

Myth 6: Bitcoin Has No Utility

Many Bitcoin skeptics view money solely through the lens of its use as a medium of exchange. However, Bitcoin has several inherent properties that provide utility. Firstly, Bitcoin is the most secure database in history. A publicly accessible database with ultimate security and immutability offers many use cases, the foremost being Bitcoin the monetary system. Regulated, day-to-day use-cases for Bitcoin have increased in the last several years. In addition to trading and long-term investing, bitcoin is accepted as a payment method with a growing number of merchants and stores. It also shows potential as an option for debt collateral. In addition, Visa is developing a credit card that offers bitcoin rewards.

Myth 7: Bitcoin Will Never Integrate With The Current Financial System

Bitcoin has already proved capable of integrating with our financial system. It is regulated as an investment asset, with the corresponding tax and reporting requirements for individuals and corporations. Bitcoin is a viable payment method with many merchants, no different than fiat currencies. Several companies now allow bitcoin to be invested in retirement accounts, and Bitcoin derivatives populate the stock market.