

ZETECH UNIVERSITY

UNIT NAME: BLOCK CHAIN TECHNOLOGY



UNIT CODE: BCE 413

LESSON 4 Introduction to Bit Coin Block Chain

- What is Bitcoin?
- What gives Bitcoin value?
- How do I create a Bitcoin wallet?
- How to buy and sell bitcoin?
- How to send bitcoin?
- How to receive bitcoin?
- How does a bitcoin exchange work?
- Bitcoin debit cards
- What are the tax implications of using Bitcoin?
- What is Bitcoin mining?
- What's a self-custodial Bitcoin wallet?
- How does Bitcoin governance work?

What is Bitcoin?

Bitcoin is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network. Bitcoin transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a block chain.

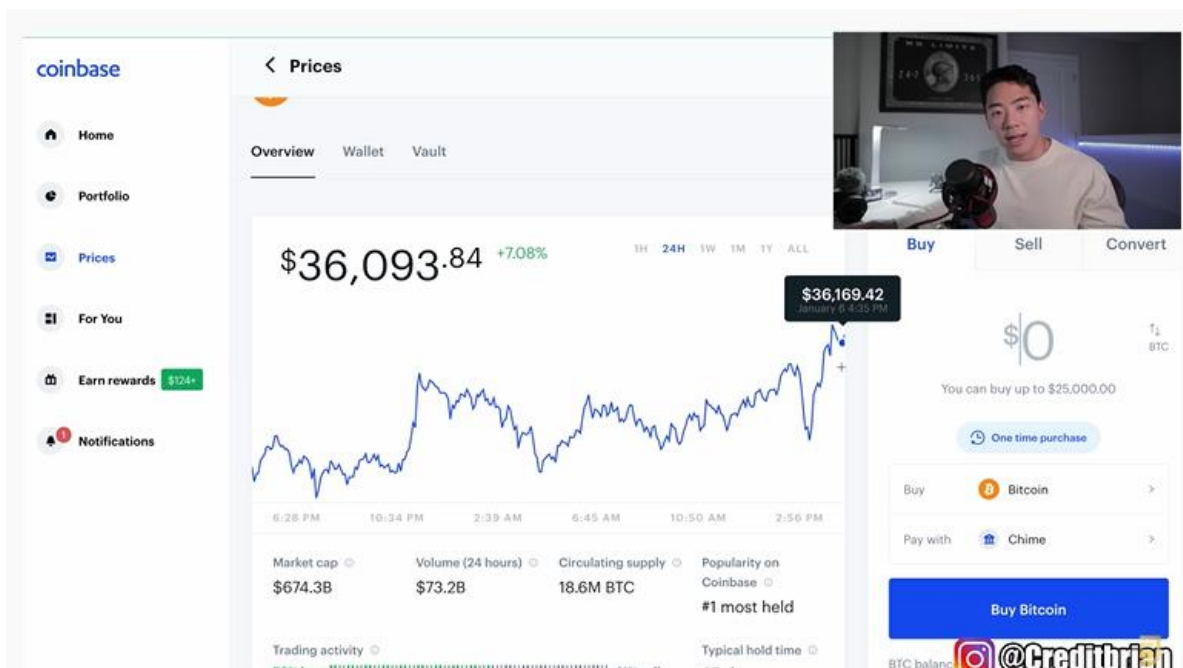
- **Code: BTC, XBT** *The abbreviation "XBT" comes from the International Standards Organization (ISO) that maintains a list of internationally recognized currencies.*
- **Exchange rate: Floating** *-A floating exchange rate is one that is determined by supply and demand on the open market.*
- **White paper: "Bitcoin: A Peer-to-Peer Electronic Cash System"**
- **Block reward: ₿6.25**
- **Circulating supply: ₿18,925,000**
- **Hash function: SHA-256 (two rounds)**
- **Symbols: BTC, ₿, ₿**
-  Bitcoin (BTC) is a cryptocurrency developed in 2009 by Satoshi Nakamoto, the name given *to its unknown creator (or creators).*
-  Transactions are recorded in a blockchain, which shows the transaction history for each unit and proves ownership.

What is Bitcoin & Cryptocurrency? We explain Video Link.

https://www.youtube.com/watch?v=0QrAdF0eE_0

How To Invest In Crypto Full Beginners Guide in 2022

<https://www.youtube.com/watch?v=Yb6825iv0Vk&t=526s>



The screenshot shows a video recording of a man in a white shirt speaking into a microphone. The background of the video is a Bitcoin price chart. Overlaid on the right side of the video is a Coinbase 'Buy' interface. The interface shows a purchase amount of \$5000, with options for 'One time purchase', 'Buy' (Bitcoin), and 'Pay with' (Chase). A 'Preview Buy' button is visible. Below the video, a blue banner reads 'How To Invest In Crypto Full Beginners Guide in 2022'. At the bottom right, there is an Instagram handle '@Creditbrian'.

Volume (24 hours) \$73.2B Circulating supply 18.6M BTC Popularity on Coinbase #1 most held

10:34 PM 2:39 AM 6:45 AM 10:50 AM 2:56 PM

Buy Sell Convert

\$5000 BTC

One time purchase

Buy Bitcoin

Pay with Chase

Preview Buy

BTC balance

@Creditbrian

How To Invest In Crypto Full Beginners Guide in 2022

This screenshot shows the same video of the man speaking, but the Coinbase interface on the right has changed to a confirmation screen. It features a blue circular icon with a white checkmark and the text 'Your order was submitted'. Below this, it says 'We will send you an email when your order status updates.' and a 'Done' button. The background Bitcoin chart and the video banner remain the same. The Instagram handle '@Creditbrian' is still present at the bottom right.

95

10:34 PM 2:39 AM 6:45 AM 10:50 AM 2:56 PM

Volume (24 hours) \$73.2B Circulating supply 18.6M BTC Popularity on Coinbase #1 most held

Typical hold time

Your order was submitted

We will send you an email when your order status updates.

Done

BTC balance 0 BTC = \$0.00

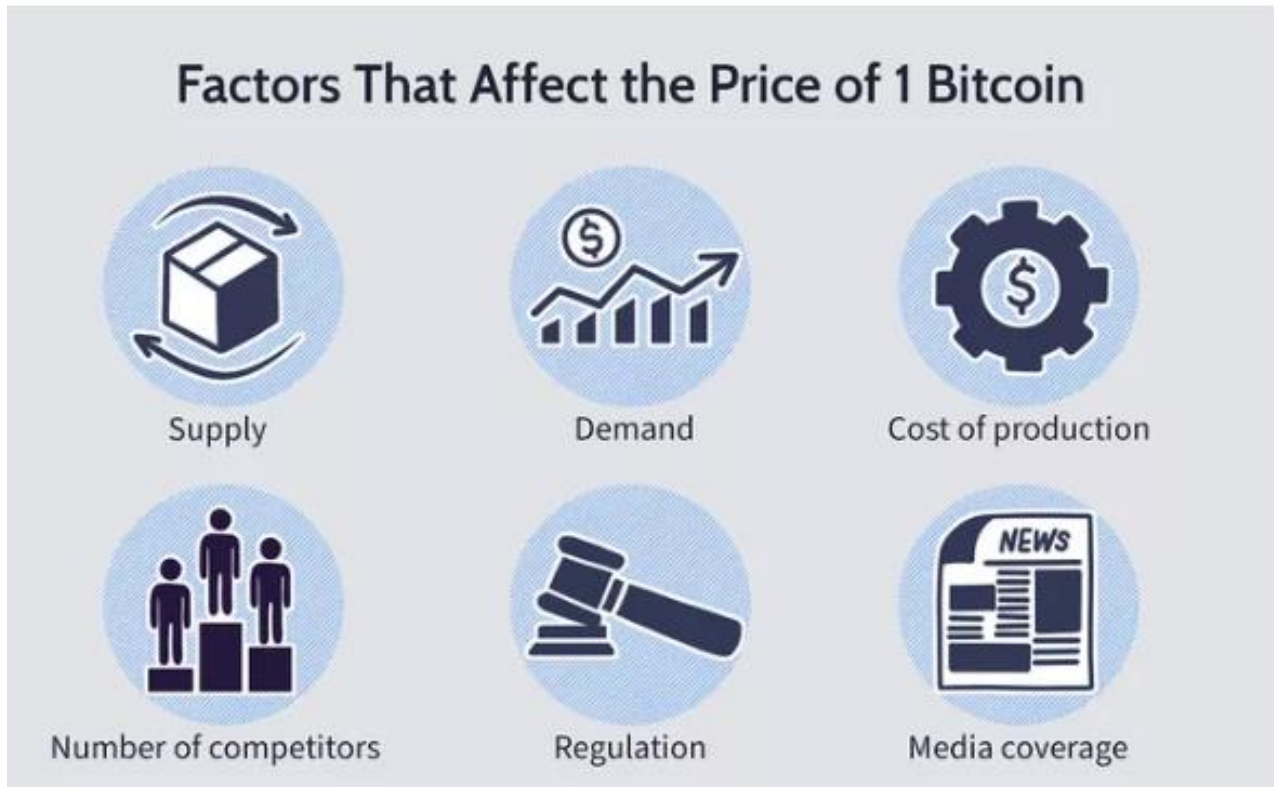
@Creditbrian

2. What gives Bitcoin value?

A Bitcoin's main source of value is its restricted supply and increasing demand. Its supply is programmed to be limited.

FAST Fast.

- The rate at which Bitcoin is created is reduced about every four years. This is called a **halving**, where the number of coins given as a reward for successfully mining a block is cut in half, the last of which was in May 2020.

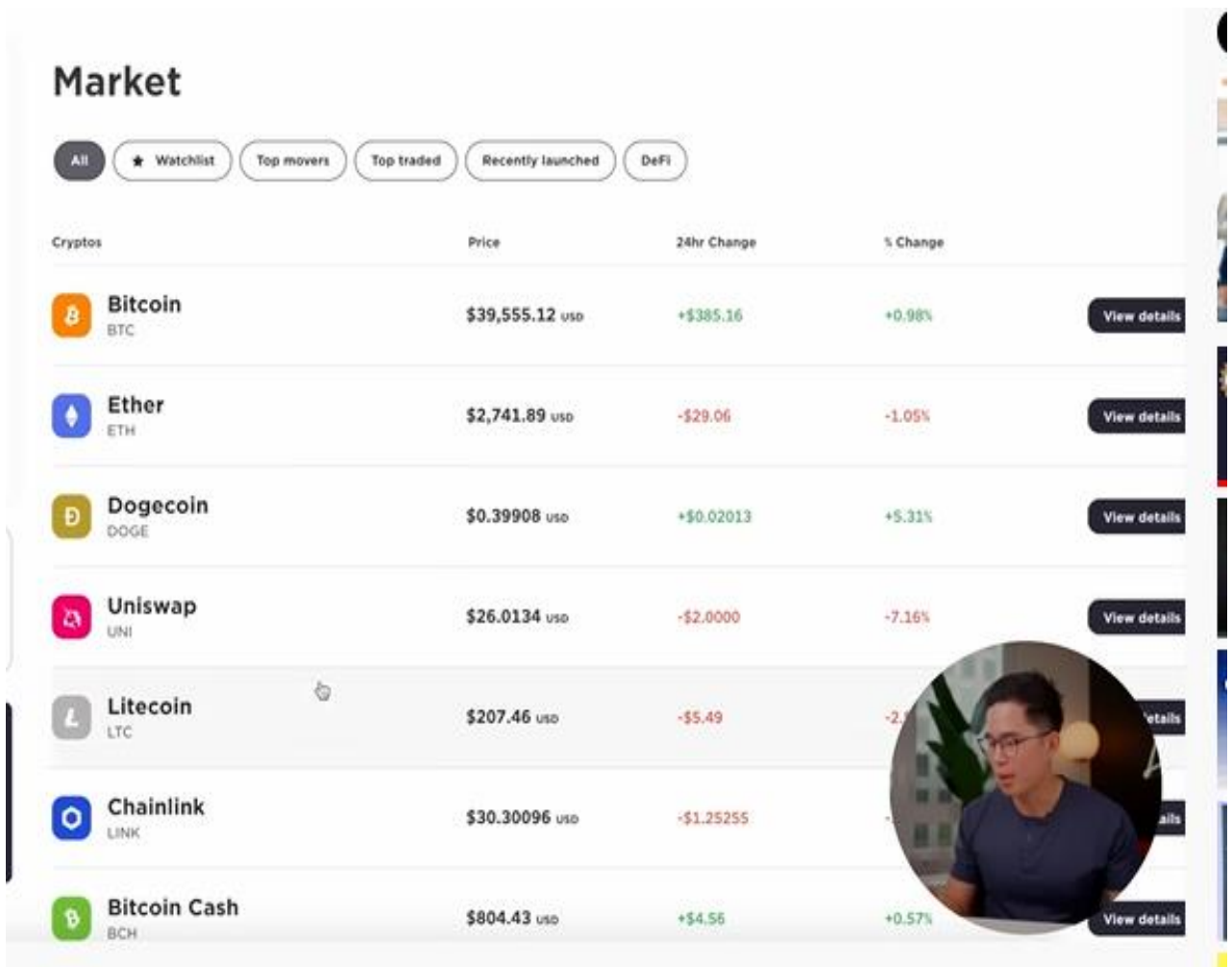









Bitcoin is often compared to gold because it has similar characteristics. Namely:

1. It **has a limited supply**. *There will only ever be 21 million bitcoins.*
2. It's **easily divisible**. *You can divide one bitcoin into 100 million pieces.*
3. It's **durable**. *A huge globally distributed network of independently operated computers tracks Bitcoin ownership. This ensures that no bitcoin is lost.*

How do I create a Bitcoin wallet?

A Bitcoin wallet is a tool for interacting with the Bitcoin network. **Use it to buy, sell, send, receive, and trade bitcoin.** Making a Bitcoin wallet is as easy as downloading an app.



Market				
All ★ Watchlist Top movers Top traded Recently launched DeFi				
Cryptos	Price	24hr Change	% Change	
 Bitcoin BTC	\$39,555.12 USD	+\$385.16	+0.98%	View details
 Ether ETH	\$2,741.89 USD	-\$29.06	-1.05%	View details
 Dogecoin DOGE	\$0.39908 USD	+\$0.02013	+5.31%	View details
 Uniswap UNI	\$26.0134 USD	-\$2.0000	-7.16%	View details
 Litecoin LTC	\$207.46 USD	-\$5.49	-2.5%	View details
 Chainlink LINK	\$30.30096 USD	-\$1.25255	-3.9%	View details
 Bitcoin Cash BCH	\$804.43 USD	+\$4.56	+0.57%	View details

How to buy and sell bitcoin?

Apps like the [Bitcoin.com Wallet](#).

Websites like the buy/sell section at [Bitcoin.com](#).

Peer-to-peer services like [Bitcoin.com Local](#).

Centralized crypto exchanges. Caution: this option is custodial.

Here's a quick video demonstrating how to send Bitcoin in the [Bitcoin.com Wallet](#):

<https://www.youtube.com/watch?v=6O7nS5-AY3Y&t=42s>

IMPORTANT: Bitcoin transactions are irreversible, so if you send to the wrong address, you'll most likely never see that bitcoin again.

How to Buy & Sell Bitcoin/Crypto via P2P on Binance for Beginners

<https://www.youtube.com/watch?v=Ktd0ywEYk44>

How to send bitcoin securely?

- Sending bitcoin is as easy as choosing the amount to send and deciding where it goes.
- The exact procedure for doing so will depend on the type of Bitcoin wallet you're using, but the main thing you need to know is the 'address' of the recipient.
 - 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
- One way to send bitcoin, then, *is to simply copy the recipient's address to your clipboard, then paste it in the send field of the Bitcoin wallet app you're using*
- Bitcoin *addresses can also be displayed in QR code format*. If you're sending bitcoin from a mobile wallet like the Bitcoin.com Wallet, you can use your phone's camera to scan the QR code of the address you want to send to. This will automatically fill in the address.

Bitcoin.com Wallet: How to send Bitcoin

<https://www.youtube.com/watch?v=6O7nS5-AY3Y&t=1s>

How does a bitcoin exchange work?

- ✓ Bitcoin exchange is the process of trading bitcoin for local currencies, goods or services, or other cryptocurrencies.
- ✓ Your options range from peer-to-peer exchange to giant centralized exchange services that resemble a stock trading account.
 - **Bitcoin is the most liquid of all cryptocurrencies as it combines the highest number of market participants with the greatest volume of exchange.** *The daily exchange of bitcoin is measured in the tens of billions of dollars!* Still, compared to cash, it's not liquid, particularly when it comes to using it to buy something in the real world.
 - For this reason, **there's a need for bitcoin exchanges.**

there's a need for bitcoin exchanges.

- When most people speak of **bitcoin exchanges**, *they're referring to centralized 'custodial' platforms like Coinbase, Kraken, and Binance.*
 - These platforms facilitate the trade of bitcoin and many other cryptocurrencies. Similar to platforms for trading stocks like

Robinhood and Charles Schwab, cryptocurrency exchanges match buyers and sellers.

- Critically, by definition, a centralized cryptocurrency exchange takes custody of your bitcoin.
 - This has a number of implications relating to security, but also relating to the freedom you have to use your bitcoin as you wish.
 - Read more on: Custodial versus non-custodial Bitcoin wallets.

What's a banked exchange?

- Cryptocurrency exchanges *that allow you to transfer local currency to and from them are known as 'banked exchanges.'* Some exchanges allow you to transfer local currency to start buying (typically in the form of credit card or payment app like PayPal), but don't allow you to withdraw local currency back to your credit card or payment app. These are known as 'partially banked' exchanges. A fully-banked exchange will allow you to fund your account via bank transfer and send local currency back to your bank account.

How do centralized bitcoin exchanges make money?

In a word: fees. These may include some or all of the following:

1. Withdrawal fees

Most exchanges charge a fee to withdraw bitcoin, other cryptocurrencies, and local currencies. In most cases, the fee is on a per withdrawal basis (not a percentage of the withdrawal amount). The withdrawal fees charged by exchanges tend to change frequently, often without notice.

NB: Bitcoin transactions incur a small fee which is paid to the miners that confirm them. Transactions with higher fees attached to them are picked up sooner by miners (who optimize for profitability)

- ✚ Fees are measured in satoshis/byte. A satoshi is the smallest divisible unit of bitcoin, which is 0.00000001 BTC (a hundred millionth of a bitcoin).

Each transaction is made up of data, which is measured in bytes. More complicated transactions involve more data and so are more expensive. Generally speaking, this means higher value transactions (involving more bitcoin) consume more data, and so require higher transaction fees. However, it's not exactly that simple.

In fact, it's entirely possible for a 1 BTC transaction to involve more data (and therefore require higher fees) than a 0.5 BTC transaction. To understand why, we need to look in some detail at how the Bitcoin blockchain actually works.

The system runs on what's known as the Unspent Transaction Output (UTXO) model, which is an efficient and privacy-enhancing way to manage the Bitcoin ledger. It works like this:

At first, coins are minted through the mining process.

These new coins form what's known as the 'coinbase.' Now imagine a miner, who has received the current 6.25 BTC block reward, sends 1 BTC to Alice. On the ledger, this actually appears as 6.25 BTC sent to Alice and 5.25 BTC sent back to the miner, leaving Alice with a balance of 1 BTC and the miner with a balance of 5.25 BTC (the miner has an unspent transaction output of 5.25 BTC). The system is analogous to paying for something using a cash note: if the cost of the item is \$2.50, you don't cut a five-dollar note in half. Instead, you hand over the whole five-dollar note and receive \$2.50 in change.

In our example, the miner has sent over a 6.25 BTC 'note' and received 5.25 BTC in change. As it relates to fees, even though the amount of Bitcoin involved is significant, the fee for completing the transaction will be relatively small because the transaction is relatively simple. That's because there's only one output (1 BTC to Alice) and it comes from only one input or 'note' (the 6.25 BTC coinbase transaction). If we think of notes as taking up space on the Bitcoin ledger, we can see that this transaction takes up the least amount of space (bytes) possible.

2. Trading fees

These are typically calculated as a percentage of the trade value and often depend on whether you're the maker or the taker (see above for an explanation of makers and takers). In most cases, makers pay lower fees than takers. The rationale for the discrepancy is that makers provide liquidity (and should, therefore, receive a discount), while takers remove liquidity (and should, therefore, be charged extra).

3. Interest/Borrowing/Liquidation Fees

Some exchanges offer margin trading. This is where you borrow to increase your position, creating what's known as leverage. Exchanges that offer margin trading typically charge additional fees based on the amount borrowed and an interest

rate determined by the total supply of funds available to all traders. You'll also likely be charged an additional fee if your position is liquidated.

Isn't Bitcoin supposed to be peer-to-peer cash? Why would I need a credit card?


Bitcoin debit cards are like prepaid credit cards.

- While Bitcoin enables people to transact peer-to-peer, this feature can only be taken advantage of within the network itself. *If your local furniture store doesn't accept bitcoin, you'll have to pay via another method!* Further, Bitcoin (at least in its current state on 'layer one') *isn't particularly useful as a medium of exchange for small-value items like your morning coffee or daily groceries.* Why?

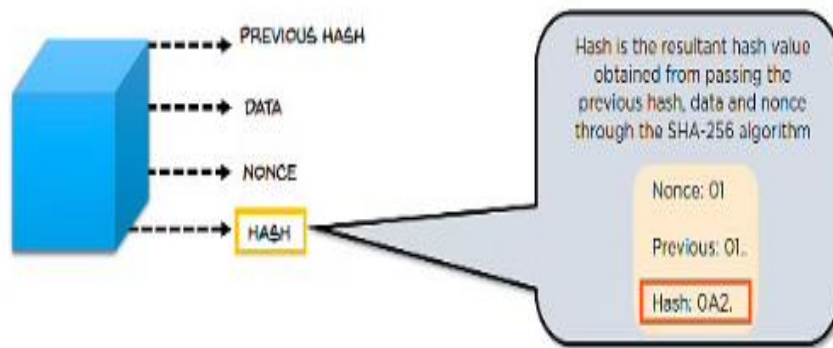
(1) **Transaction fees** - are often significantly higher than with status quo payment networks like **Visa** and **Mastercard**.

(2) **Transaction times are significantly longer than with status quo payment networks.** Depending on the fees paid and the current level of network congestion, it takes anywhere from a few minutes to an hour for most Bitcoin transactions to confirm 'on chain' - and only when a transaction is confirmed on chain, meaning it's included in at least one block, can final settlement be considered to have occurred.

What is Bitcoin mining?

 **Bitcoin mining** - *is the process of creating new bitcoins/to record current bitcoin transactions in blocks, by solving extremely complicated math problems that verify transactions in the currency.*

- *Bitcoin miners use software to solve transaction-related algorithms that check bitcoin transactions. In return, miners are awarded a certain number of bitcoin per block.*
- ✓ *The process of bitcoin mining involves the verification of new transactions against the Bitcoin network, which results in the production of new bitcoins.*
- ✓ *Bitcoin mining is the process by which Bitcoin transactions are validated digitally on the Bitcoin network and added to the blockchain ledger.*
- ✓ *It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralized blockchain ledger.*



How long does it take to mine 1 bitcoin? **about 10 minutes**

- In general, it takes about 10 minutes to mine a block, and a block will award a number of coins to whoever mines it. Unfortunately, because of the sheer number of people mining coins solo miners are a rarity because the odds of being the one to discover a block are very low.

Bitcoin vs. Traditional Currencies

While both Bitcoin and traditional currency are similar in that both are a store of value, they differ in many ways.

Some differences between Bitcoin and traditional currencies are illustrated in the table below.

	Bitcoin	Traditional Currency
Tangibility	It is a virtual currency and can only be used in its digital form	It is a physical currency in the form of notes and coins. However, we can use it in both physical and digital forms

Regulation	Issued through mining and controlled by a decentralized distributed network of computers	Issued and controlled by central government authorities, i.e., central banks. Owing to this, the traditional currency is the legal tender in the country governed by the issuing authority.
Governance	Governed by a consensus mechanism in which the majority rules	Purely governed by the central bank
Value	Value is backed by the trust of its users. The more users are willing to transact with Bitcoin, the more stable it becomes.	Value is determined by forces of supply and demand and is thus vulnerable to inflation
Supply	Capped at 21 million bitcoin	Fiat currency has no supply limit
Validation of transactions	Bitcoin transactions are validated using blockchain technology and so do not require an intermediary for validation	Transactions involve an intermediary such as a bank or a payment provider
Transaction fees	Minimal or no associated fees as intermediaries have been eliminated	Transactions attract considerable charges

Transaction time and speed	The transaction is almost always instantaneous or greatly depends on the network speed	Transactions may take time before verification or before they reflect on the system
Security	The concepts of decentralization, cryptography, and consensus guarantee a secure network and security of bitcoin transactions	Less secure as it can be negatively affected by fluctuations in government policies
Reversals	Bitcoin transactions cannot be charged back, reversed, or canceled	Chargebacks, reversals, and cancellations are commonplace with traditional currency transactions

Here is a breakdown of what happens during bitcoin mining

- The Mining Requirements

A bitcoin miner will first select their tools of the trade and set them up. These include:

- ✓ Hardware GPU (graphics processing unit), SSD for crypto mining, or ASIC (application-specific integrated circuit)
- ✓ Mining software
- ✓ A **wallet a software program that** (keeps your private keys – the passwords that give you access to your cryptocurrencies – safe and accessible, allowing you to send and receive)
- ✓ Preferred mining pool (if one chooses pool mining option instead of solo mining)

For every transaction input, a bitcoin mining software generates a unique cryptographic hash puzzle that is difficult to decode. The software then groups the number of transactions required to form a **block into a Merkle tree.**

✚ The Merkle tree enables the efficient verification of transactions in the bitcoin network.

The Merkle Tree and the SHA-256 Algorithm

- A Merkle tree is a data structure of the hashes in a block and acts as a summary of all the transactions in the block.
- In the Merkle tree, hashes of individual transactions known as transaction IDs are paired repeatedly using the SHA-256 algorithm until only one hash identifies the entire tree. This hash is known as the Merkle root or root hash.

Class Assignment 1

1. What is Merkle Tree data structure? And its relevance in BLOCK CHAIN TECHNOLOGY. How its computed and applied. (10 marks)