UNIT - 2

Bitcoin: Basics, Creation/Projections of Coins, Double‑spending attack, Bitcoin Anonymity, Basics of Bitcoin Script (FORTH), Bitcoin transactions through script.

What is Bitcoin?

There are a number of currencies in this world used for trading amenities. Rupee, Dollar, Pound Euro, and Yen are some of them. These are printed currencies and coins and you might be having one of these in your wallet. But bitcoin is a currency you can not touch, you can not see but you can efficiently use it to trade amenities. It is an electronically stored currency. It can be stored in your mobiles, computers, or any storage media as a virtual currency.

Bitcoin is an innovative digital payment system. It is an example of a cryptocurrency and the next big thing in finance.

It is a virtual currency designed to act as money and outside the control of any person or group thus eliminating the need for third-party in financial transactions. It is used as a reward for the miners in bitcoin mining. It can be purchased on several exchanges.

Features:

- Distributed: All bitcoin transactions are recorded in a public ledger known as the blockchain. There are nodes in the network that maintain copies of the ledger and contribute to the correct propagation of the transactions following the rules of the protocols making it impossible for the network to suffer downtime.
- Decentralized: There is no third party or no CEO who controls the bitcoin network. The network consists of willing participants who agree to the rules of a protocol and changes to the protocol are done by the consensus of its users. This makes bitcoin a quasi-political system.

- Transparent: The addition of new transactions to the blockchain ledger and the state of the bitcoin network is arrived upon by consensus in a transparent manner according to the rules of the protocol.
- Peer-to-peer: In Bitcoin transactions, the payments go straight from one party to another party so there is no need for any third party to act as an intermediary.
- Censorship resistant: As bitcoin transactions are pseudo-anonymous and users possess the keys to their bitcoin holdings, so it is difficult for the authorities to ban users from using their assets. This provides economic freedom to the users.
- Public: All bitcoin transactions are available publicly for everyone to see. All the transactions are recorded, which eliminates the possibility of fraudulent transactions.
- Permissionless: Bitcoin is completely open access and ready to use for everyone, there are no complicated rules of entry. Any transaction that follows the set algorithm will be processed with certainty.
- Pseudo-anonymous: Bitcoin transactions are tied to addresses that take the form of randomly generated alphanumeric strings.

Drawbacks of Bitcoin

- Volatility: There are various factors that contribute to bitcoin's volatility like uncertainty about its future value, security breaches, headline-making news, and one of the most important reasons is the scarcity of bitcoins. It is known that there is a limit of 21 million bitcoins that could ever exist which is why some regard bitcoin as a scarce resource. This scarcity makes bitcoin's price variable.
- No government regulations: Unlike the investments that are done through central banks, bitcoins transactions are not regulated by any central authority due to a decentralized framework. This means that bitcoin's transactions don't come with legal protection and are irreversible which makes them susceptible to crimes.
- No buyer protection: If the goods are bought using bitcoins and the seller does not send the promised goods then nothing can be done to reverse the transactions and since there is no central authority so no legal protection can be provided in this case.

- Not widely accepted: Bitcoins are still only accepted by a small group of online merchants. This makes it infeasible to rely completely on bitcoin as a currency and replace it with traditional bank transactions.
- Irreversible: There is a lack of security in bitcoin transactions due to the anonymous and non-regulated nature of the bitcoin transactions. If the wrong amount is sent or the amount is sent to the wrong recipient then nothing can be done to reverse the transactions.

Youtube Video :

▶ What is Bitcoin? (v1)

▶ What is Bitcoin? Explained in 3 Minutes | Tuttle Twins

▶ Bitcoin explained and made simple

Creation of Bitcoins (Mining)

Bitcoin mining is the process by which new bitcoins are created and transactions are validated and added to the blockchain.

How it Works:
Miners use powerful computers to solve complex cryptographic puzzles (Proof of Work).The first miner to solve the puzzle adds a new block to the blockchain.As a reward, the miner receives a fixed number of bitcoins — this is how new bitcoins are created.

Block Reward and Halving:
Initially, each block gave a reward of 50 BTC. Every 210,000 blocks (~every 4 years), the reward is halved (known as Bitcoin Halving).

Year	Block Reward (BTC)
2009	50
2012	25
2016	12.5

2020	6.25
2024	3.125
~2028	1.5625

Projections of Bitcoin Supply

Maximum Supply:
Bitcoin has a fixed supply limit of 21 million coins. As of mid-2025, over 19.7 million bitcoins have already been mined.It is projected that the last bitcoin will be mined around the year 2140.

Year	Estimated BTC in Circulation
2025	~19.7 million
2032	~20.4 million
2040	~20.9 million
2100	~20.99 million
2140	21 million (maxed out)

Youtube Video :

What is Bitcoin Mining for Beginners - Short and Simple

Double Spending Attack

What is Double Spending?

Double spending means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flaw that allows users to duplicate money. Since digital currencies are nothing but files, a malicious user can create multiple copies of the same currency file and can use it in multiple places. This issue can also occur if there is an alteration in the network or copies of the currency are only used and not the original one. There are also double spends that allow hackers to reverse transactions so that transaction happens two times. By doing this, the user loses money two times, one for the fake block created by the hacker and for the original block as well. The hacker gets incentives as well for the fake blocks that have been mined and confirmed.

The Double Spending Problem

- Initial Transaction: Alice has 1 Bitcoin (BTC). She decides to send 1 BTC to Bob. This transaction is broadcast to the network and is pending confirmation.
- Attempt to Double Spend: While the transaction to Bob is still pending, Alice tries to spend the same 1 BTC again. She creates a second transaction, sending the same 1 BTC to Charlie. This second transaction is also broadcast to the network.
- Network Propagation: The two transactions (to Bob and Charlie) are now competing to be included in the blockchain. Each transaction is seen by different nodes in the network, and there may be a delay in the entire network agreeing on which transaction is valid.
- Block Confirmation: The network eventually confirms one of the transactions (e.g., the transaction to Bob). This transaction is added to a block in the blockchain, making it permanent.
- Conflict Resolution: If the transaction to Bob is confirmed first, the network sees that Alice has already spent the 1 BTC, so the transaction to Charlie is invalidated. If the transaction to Charlie somehow gets confirmed first, Bob's transaction will be rejected.
- Final Outcome: The blockchain only records one transaction because it is designed to prevent double-spending. The system resolves the conflict by ensuring that only one of Alice's transactions is valid.

How Does Double Spending Happen?

- Multiple Transactions: An attacker might attempt to make two separate transactions with the same amount of digital currency. If the system doesn't quickly and accurately update transaction records, both transactions might initially appear valid.

- Network Delay: In decentralized systems like blockchain, there is a delay between when a transaction is broadcast and when it is confirmed by the network. During this time, an attacker could try to spend the same digital currency in another transaction.
- Fraudulent Techniques: Attackers might use techniques such as:
  - Race Attack: Sending conflicting transactions to different nodes to exploit the delay in transaction propagation.
  - Finney Attack: Pre-mining a block with a conflicting transaction and then spending the same funds before the pre-mined block is added to the blockchain.
  - 51% Attack: Gaining control of more than half of the network's computing power to reverse or alter transactions.

Youtube Video : What is Double Spending
Bitcoin 51% Attack EXPLAINED in 3 minutes
Crypto: How Satoshi Nakamoto Solved The Double Spending Problem [Explain…

What is Bitcoin Anonymity?

People often say Bitcoin is anonymous, but this is not fully true.Bitcoin is actually pseudo-anonymous — which means Your name is not shown on the Bitcoin network, but your Bitcoin address and all transactions are public.

Example :
You have a Bitcoin wallet with this address: 1A2b3C4d5E6F7g8H9iJ0kLmN

Now you send 0.5 BTC to your friend.

The blockchain shows:

- Your wallet address
- Friend's wallet address
- Amount: 0.5 BTC
- Date & Time of transaction

But it does not show your name or personal info.

So, Are You Anonymous?
Yes – if no one knows that address belongs to you.
No – if you used that address on an exchange or app that has your real name (like KYC).

Is Everything Public?
Yes. The Bitcoin blockchain is like a public diary.

Anyone in the world can:

- Search your address
- See how much Bitcoin you sent or received
- Track your past transactions

Can Someone Trace You?
Yes, using these:

- Your address from a crypto exchange (which knows your name)
- IP address while sending coins
- Patterns in how you use Bitcoin

Companies like Chainalysis help governments and banks trace Bitcoin users.

Summary

Question	**Answer**
Is Bitcoin anonymous?	❌ No (it's pseudo-anonymous)
Can people see your transactions?	✅ Yes, all are public
Can your identity be found?	✅ Yes, if someone links your address
Is Bitcoin good for privacy?	😐 Somewhat, but not fully private
Can privacy be improved?	✅ Yes, with special tools or methods

Basics of Bitcoin Script (FORTH)

Forth is a stack-based, postfix (Reverse Polish Notation) programming language. It's different from C-like languages in that it uses a data stack for computation and avoids traditional syntax (no if, while, or even = in the usual sense).

Example 1: Pushing and Adding

```
3 4 + .
```

Explanation:

- 3 → pushes 3 onto the stack
- 4 → pushes 4 onto the stack
- + → pops the top two values (3 and 4), adds them (7), and pushes the result back
- . → pops and prints the top value (which is 7)

Output : 7

Operator	Description
+	Add top two items
-	Subtract
*	Multiply
/	Divide
mod	Remainder

Example :

```
10 3 mod .
```

Output : 1

If you just want to see the stack, .s will be used.

Example : 1 2 3 .s

Output : <3> 1 2 3   This shows the stack contains 3 items: 1, 2, and 3 (bottom to top).

Word	Description
dup	Duplicate top of stack
drop	Remove top item
swap	Swap top two items
over	Copy second item and push on top

Example	Output
1 2 dup .s	1 2 2
1 2 swap .s	2 1
1 2 over .s	1 2 1
1 2 drop .s	1
Practice Following Examples	
5 6 swap .s	6 5
3 4 over + .s	3 7
9 dup * .	81

Syntax for Defining a Word

```
: word-name   code-here   ;
```

- : begins the definition.
- word-name is the name of your new word.
- code-here is what it does.
- ; ends the definition.

Example	Output
: say-hello ." Hello, Forth!" ; say-hello	Hello, Forth!
: add-two + . ; 5 6 add-two	11
: square dup * ; 4 square .	16
: cube dup dup * * ; 3 cube .	27

Control Structures in Forth (IF, ELSE, THEN, BEGIN...UNTIL, DO...LOOP)

Syntax :

:word condition IF true-part ELSE false-part THEN

Example	Output
: check-positive (n --) 0 > IF ." Positive" ELSE ." Not Positive" THEN ; 5 check-positive	Positive
: even-odd (n --) 2 mod 0= IF ." Even" ELSE ." Odd" THEN ; 4 even-odd	Even

Online Tool : Here

Learn forth in details here

Learn Script in details Here

Youtube Video : Bitcoin Lesson | Script