

UNIT-3

Introduction to Bitcoin:

- ⇒ Bitcoin chain and scripts
- ⇒ use cases of Bitcoin Blockchains
- ⇒ scripting language in micro payment
- ⇒ escrow etc downside of Bitcoin mining
- ⇒ Block chain science:
 - ⇒ Grid coin
 - ⇒ Folding coin
 - ⇒ Block chain Economics
 - ⇒ Bit coin noobs.

Bitcoin chain and scripts:-

⇒ Bitcoin script is a simple, stack-based Programming Language that enables the processing of transactions on the Bitcoin Blockchain.

⇒ Script is a Forth-like, stack-based, reverse-polish, Turing incomplete Programming language.

⇒ Script itself is implemented using the Programming Language the Bitcoin software is written in.

⇒ The original implementation of the Bitcoin software was written in C++.

⇒ Script was implemented by satoshi Nakamoto.

Stack-based:-

⇒ Bitcoin -script uses a data structure that can be thought of as a linear structure represented by a physical stack.

⇒ Items at the top of the stack can be added (pushed) or removed (popped) in a "Last in, First out (LIFO)" queue.

Forth - Like:-

⇒ Script resembles Forth, a Programming Language that first appeared in 1970.

⇒ Forth is used in the open firm ware

Boot loaders

Reverse - polish notation (RPN):

⇒ Also known as postfix notation, RPN is a method of placing the operation function at the end of a sentence.

Example :- Adding 5 and 6 in script must be written as "56 +" rather than "5+6".

Turing Incomplete :-

⇒ Turing incomplete means the script for Bitcoin and other ~~communication~~ cryptocurrencies does not allow infinite loops.

⇒ The turing incomplete machines can be used to solve halting problems.

version	#inputs	inputs	#outputs	outputs	lock time
4-byte	VarSize	VarSize	VarSize	VarSize	4-byte
prev-tr-id 32-byte	prev-out-index 4-byte	script length VarSize	script sig VarSize	n скрипта 4-byte	
		value 8-byte	script pub key length VarSize	ScriptPubKey VarSize	

Use cases of Bitcoin Blockchain Scripting

Language in micro payment:-

Use cases of Bitcoin Blockchain:-

→ Blockchain came into prominence with the advent of cryptocurrencies like Bitcoin, a peer-to-peer electronic money system.

Smart contracts:-

→ These programs is to automate the execution of contract terms when certain conditions are met.

Cybersecurity:-

Blockchain is highly secure because of their permanency (不可篡改), transparency and distributed nature.

IOT:-

→ IOT devices that record measurements captured by Sensors.

Cryptocurrency:-

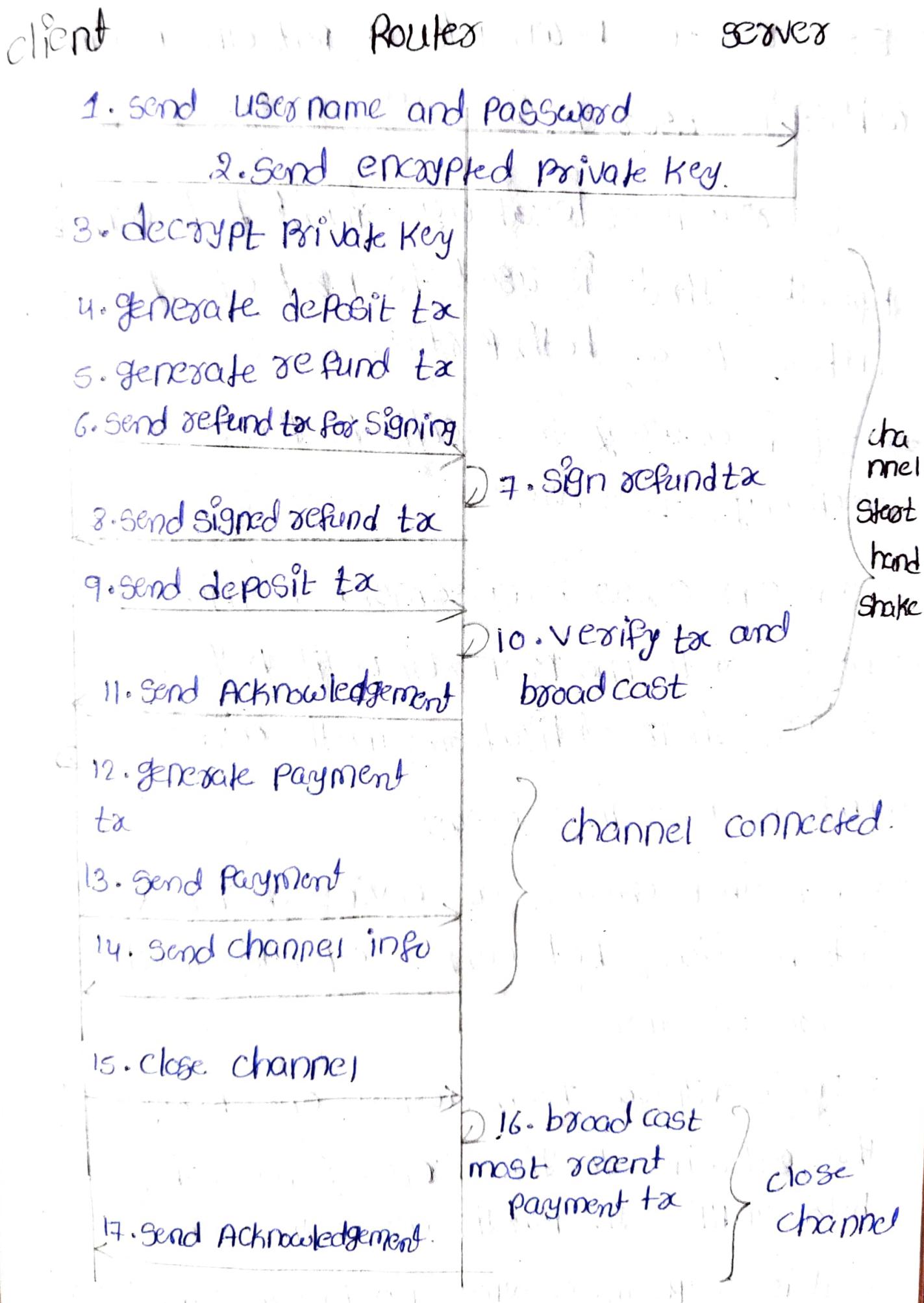
→ The blockchain technology is widely used to develop cryptocurrency such as Bitcoin.

Bitcoin micro Payments :-

- ⇒ Today a micro payment is typically defined as a amount less than one dollar.
- ⇒ We researched two alternative ways to perform micro payments on bitcoin network
 - * Directly broadcasting micropayments to the Bitcoin network
 - * Bit coin micro payment channels
- ⇒ Bit coin micro payment channels more efficient than direct broadcast

micro payment channel protocol :-

- ⇒ micro payment channel protocol consists 3 stages : channel start, channel connected, channel End.



EScrow etc Downside of Bitcoin mining:-

what is Escrow:-

- ⇒ Escrow is a legal agreement between two parties that is used to protect the interests of both parties.
- ⇒ It is a way to facilitate the secure exchange of services.
- ⇒ In an escrow agreement, a third party holds onto the property until both parties fulfill their obligations in the agreement.

what is Bitcoin Escrow:-

- ⇒ Bitcoin Escrow is a service designed an intermediary between two parties involved in a transaction.
- ⇒ In a typical transaction, one party sends the Bitcoin to the Escrow Service, where it is held until both parties agree the transaction.
- ⇒ This type of service mostly used in online transactions.
- ⇒ It provides trust and security to the transaction.

→ The purpose of using an escrow service is to protect both parties from any potential fraud.

Service Providers for Bitcoin Escrow:-

1. Paxful Escrow Service:-

→ Paxful Escrow is an online marketplace that allows users to buy and sell Bitcoins on a peer-to-peer basis.

→ It provides safe environment for trading Bitcoins.

2. Local Bitcoins:-

→ Local Bitcoins is one of the oldest Bitcoin escrow services (2012).

→ It is used by 3 million users world wide and enables them to buy and sell Bitcoin with each other directly.

3. Bitrated:-

→ Bitrated is a Bitcoin escrow service that became popular with the masses by offering enhanced security for users.

→ Bitrated's transactions can be slow at times.

4-Bisq:

⇒ Bisq is a decentralized, open-source exchange that allows users to buy and sell Bit coin directly with each other.

Block chain science :-

Grid coin:-

- ⇒ Grid coin is a unique cryptocurrency that does not rely on traditional mining for its creation.
- ⇒ It utilizes a decentralized network for volunteer computers to perform various scientific calculations.
- ⇒ Grid coin is established with a support scientific research and advancements.

How Grid coin works:-

- ⇒ Grid coin operates on the BOINC platform which stands for the "Berkeley Open Infrastructure for Network Computing".
- ⇒ BOINC act as a underlying framework that connect volunteer computers.
- ⇒ When you participate in Grid coin, your computer becomes part of a large network dedicated to scientific research.

Earning Gridcoin Tokens:-

- ⇒ one of the main incentives for individuals to participate in the Gridcoin network is the ability to earn Gridcoin tokens.
- ⇒ These tokens can be stored, traded or used to support further research within the Gridcoin ecosystem.
- ⇒ The amount of tokens earned depends on the number of computations performed by your computer to the network.

Real-world Applications:-

Gridcoin's unique approach to cryptocurrency has various practical applications.

1. Scientific Research:-

- ⇒ The primary use case for Gridcoin is scientific research.
- ⇒ Utilize the computational power of volunteer computers, Gridcoin supports a broad range of projects.

2. Climate modeling and conservation

3. medical research and drug discovery

4. Astronomy and cosmology

Folding coin:-

- ⇒ Folding coin (FLDC) is a digital token that compensates participants (folders) for their Folding@home (FAH) computational power.
- ⇒ With growing community support, more folders are consistently joining the FAH network, to help find cures for cancer, Alzheimer's and many other viral diseases.
- ⇒ Merged, Folding platform, you can earn more than just FLDC, but also other cryptocurrencies.

what is Folding @ Home:-

- ⇒ Folding@home (FAH) is a project by Stanford University that has been running since October 2000.
- ⇒ FAH use a idle computer power to help simulate how proteins fold in the human body.
- ⇒ Researchers normally have to spend millions of dollars on super computers to do these simulations.
- ⇒ With FAH and the power of the internet, the workload is broken into small work units

and sent to anyone who downloads and runs the FAH program.

what Does Folding coin Do?

- ⇒ Folding coin provides an incentive to Folders by distributing FLDC and other tokens.
- ⇒ Folders earn "points" by completing work unit in a timely manner.

Blockchain Genomics:-

- ⇒ Using genomic datasets, researchers try to extract information about the molecular mechanisms of human disease, which can help identify disease specific mutations.
- ⇒ The human genome consists 3 billion base pairs.
- ⇒ Some genetic diseases are rare, and even some common diseases.
- ⇒ The datasets require specific infrastructure and pipelines for processing.
- ⇒ The Data increase in a genetic dataset it may raise security problems so block chain to solve this problems and perform safe operations on data.

Introduction to genomics:

- ⇒ Genomics is a special field of biology that deals with the structure, function, evolution, mapping and editing of genomes.
- ⇒ A genome is a complete set of genetic information in an organism.

Blockchain in Genomics:-

- ⇒ A blockchain is a digital, decentralized public ledger designed to record every data on its network.
- ⇒ Blockchain playing a major role in health care, especially in genomic medicine.
- ⇒ This technology used by scientists will be able to gain a deeper understanding of disease mechanisms.

Why Blockchain in Genomics:

* Genomic Data Security:-

- ⇒ Genomic data is very sensitive and crucial. From data security perspective, blockchain provides excellent data security and integrity.

- ⇒ Blockchain Technology providing better protection against data breaches.
- ⇒ Blockchain uses hashing techniques to store data securely.
- * Genomic Data Sharing:-

- ⇒ The Genomic Data and blockchain network is possible to send anonymous genetic information around the world.
- ⇒ The decentralized nature of blockchain allows easy and secure data exchange between organizations.
- ⇒ The Decentralized nature of blockchain data can not be modified.
- * Immutability of genomic data:-
- ⇒ Blockchain provides immutability of genomic data per organizations, helping organizations protect information.
- ⇒ The Decentralized nature of blockchain data can be changed at one place it can reflected all nodes.

- * Efficiency:- Blockchain technology can help to make the process more efficient. It can reduce the time taken for data sharing and analysis.
- * Privacy:- Blockchain eliminate third-party intervention b/w genomic data sharing and analysis, making the system more efficient and faster.

* Cost Reduction:-

Blockchain does not require a third person it reduces costs for organizations and gives trust to other partners.

why Blockchain technology suitable for Bio-informatics and Healthcare Applications:-

- ⇒ Blockchain plays an important role in Bioinformatics and Healthcare Applications as it reduces the cost of Analysis in genomics and health Applications.
- ⇒ Transactions of data on Blockchain system are faster and more efficient than traditional processes.
- ⇒ In a Blockchain technology every transaction is more transparent and traceable.

⇒ Blockchain prevents fraud and unauthorized activity better than other systems.

Current Trends in Blockchain-Based Systems in Genomics:-

1. Proof of Concept Era (from 2016 to 2018):

⇒ The main goal of this era is to provide an efficient application to prove that the block-chain platform can be used.

2. Blockchain Development Era (from 2019 to 2020):

⇒ complex cloud-based and encryption-based applications are mainly proposed.

3. Blockchain As a platform era (from 2021 to present day):

⇒ Blockchain is converted into a platform that has additional AI-based algorithms running on the blockchain platform.

Bitcoin Moods:-

⇒ On February 5, 2021, Bitcoin Association, the Switzerland-based global industry organization that works to advance business with the Bitcoin network, announced the official launch the

massive open online course (Mooc).

- ⇒ It offers an introduction to Bitcoin as a technology - covering its system, network, protocol, blockchain and digital currency.
- ⇒ The courses, including all assessments, are offered free of charge.
- ⇒ The series of Moocs will be taught with a focus on Bitcoin SV (Satoshi's vision).