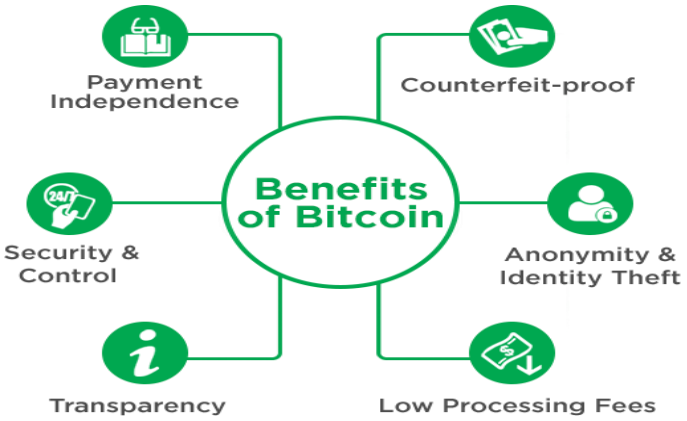
Block Chain UNIT-3 - It contains all the detailed notes

block chain technology (Jawaharlal Nehru Technological University, Kakinada)

BLOCK CHAIN TECHCNOLOGIES

UNIT-3

INTRODUCTION TO BITCOIN:



Created in 2009, Bitcoin is a digital asset that leverages a peer-to-peer network to facilitate the transfer of value without intermediation from banks or central authority. Bitcoin is a digital currency, with no physical bitcoins in circulation.

Bitcoin is a digital cryptocurrency and a groundbreaking financial innovation that was created by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. It was introduced in a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" published in 2008 and the Bitcoin network itself was launched in 2009. Bitcoin is often referred to as the first and most well-known cryptocurrency, but it's important to note that it has inspired the creation of thousands of other cryptocurrencies since its inception.

The key aspects of Bitcoin:

Digital Currency: Bitcoin is a purely digital form of currency, which means it exists only in electronic form. It is not tied to any physical commodity like gold or a government's currency like the US dollar.

Decentralized: Bitcoin operates on a decentralized network of computers, known as a blockchain. This decentralized nature means that no single entity, government, or

organization controls it. Transactions and the issuance of new Bitcoins are managed collectively by the network.

Blockchain Technology: Bitcoin's underlying technology is the blockchain, a public ledger that records all Bitcoin transactions. This ledger is maintained and updated by a distributed network of computers (nodes). The blockchain is immutable and transparent, making it highly secure and resistant to tampering.

Limited Supply: Bitcoin has a capped supply of 21 million coins. This scarcity is built into the system's code, and it's designed to control inflation and mimic some of the qualities of precious metals like gold.

Mining: The process of creating new Bitcoins and validating transactions on the Bitcoin network is called mining. Miners use specialized computer hardware to solve complex mathematical puzzles, and in return, they are rewarded with new Bitcoins and transaction fees.

Security: Bitcoin transactions are secured using cryptographic techniques. Private and public keys are used to sign and verify transactions, making it very difficult for unauthorized parties to alter or fake transactions.

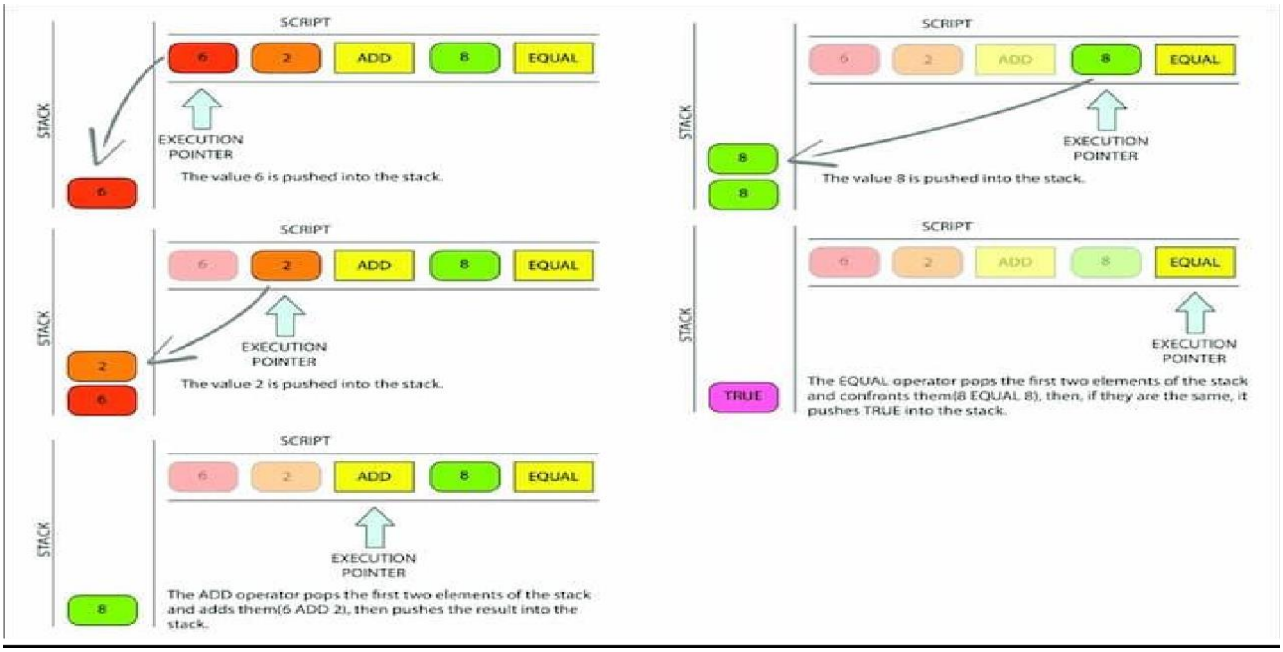
Pseudonymity: While Bitcoin transactions are recorded on the blockchain and are visible to anyone, the parties involved are represented by cryptographic addresses rather than personal information. This provides a degree of privacy, but it is not entirely anonymous.

Volatility: The price of Bitcoin can be highly volatile, with significant price fluctuations over short periods. This volatility has made Bitcoin a subject of both speculation and investment.

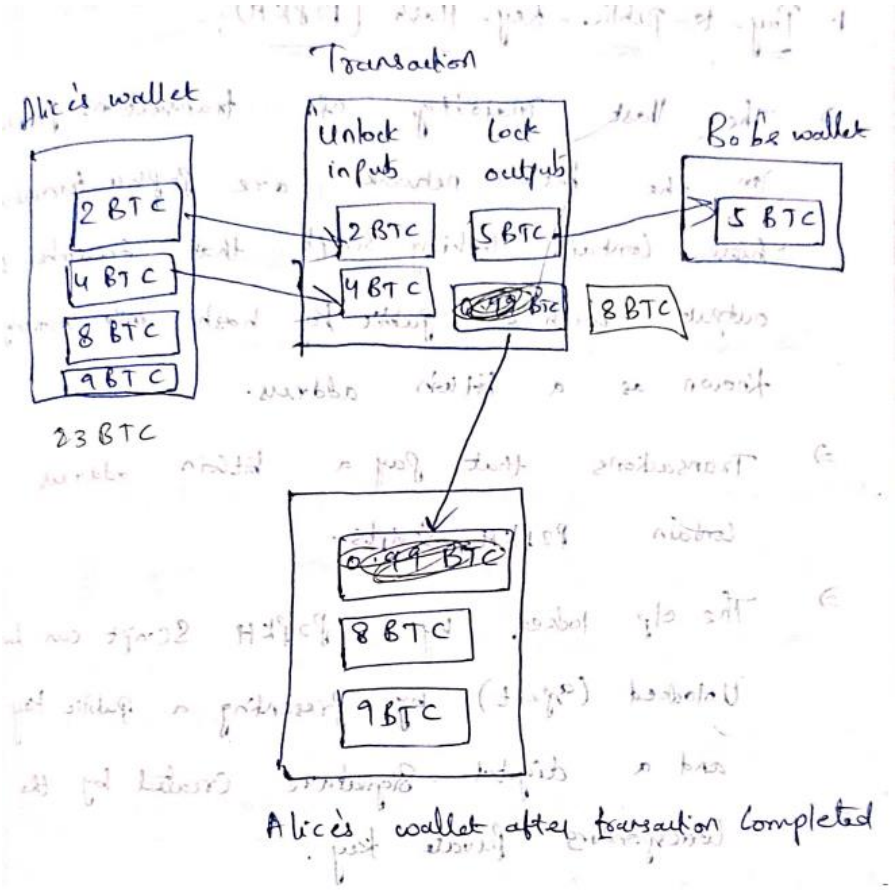
Use Cases: Bitcoin was initially conceived as a peer-to-peer electronic cash system, but it has evolved to be used for various purposes. People use it for online purchases, as a store of value, and as a speculative investment. Some see it as a potential hedge against traditional financial systems.

Global Reach: Bitcoin is accessible to anyone with an internet connection, making it a borderless form of currency. This global reach has attracted users and investors from around the world.

BITCOIN BLOCK CHAIN AND SCRIPTS:



Bitcoin Script is a lightweight programming language that is used to define the conditions under which Bitcoin transactions can be spent. It's a simple, stack-based language that can be thought of as a set of instructions that specify how Bitcoin transactions are to be processed.



Bitcoin's blockchain and scripts are fundamental components of the cryptocurrency that play crucial roles in facilitating transactions, securing the network, and enabling various advanced features.

1. Bitcoin Blockchain:
The Bitcoin blockchain is a public, decentralized ledger that records all transactions made with Bitcoin. It serves as the backbone of the network, providing transparency, security, and immutability. Here are key features of the Bitcoin blockchain:

Transaction Records: Each entry in the Bitcoin blockchain represents a transaction, including details like sender and recipient addresses, the amount of Bitcoin transferred, and a digital signature for verification.

Blocks: Transactions are grouped into blocks, typically containing a set number of transactions. These blocks are linked together in a chain, hence the term "blockchain." New blocks are added to the blockchain at regular intervals through a process known as mining.

Mining: Mining involves solving complex cryptographic puzzles to validate transactions and create new blocks. Miners compete to solve these puzzles, and the first to succeed gets to add a new block to the blockchain. In return, miners are rewarded with newly created Bitcoins and transaction fees.

Decentralization: The Bitcoin blockchain is maintained by a decentralized network of nodes, each of which stores a copy of the entire blockchain. This decentralized nature makes it highly resistant to censorship and tampering.

Immutability: Once a block is added to the blockchain, it is extremely difficult to alter the information within it, thanks to the cryptographic hashing of each block and the fact that subsequent blocks depend on the previous ones. This immutability is a key feature of blockchain technology.

2. Bitcoin Scripts:

Bitcoin scripts are a scripting language used to define the conditions under which a Bitcoin transaction can be spent. They enable the implementation of complex conditions and smart contracts within the Bitcoin network. Here are some important aspects of Bitcoin scripts:

ScriptPubKey: This is a script attached to an output when Bitcoins are sent to an address. It specifies the conditions that must be met for those Bitcoins to be spent in a future transaction. Common script types include Pay-to-Public-Key-Hash (P2PKH) and Pay-to-Script-Hash (P2SH).

ScriptSig: When a user wants to spend Bitcoins received at a specific address, they provide a ScriptSig that, when combined with the corresponding ScriptPubKey, must evaluate to true according to the Bitcoin script rules.

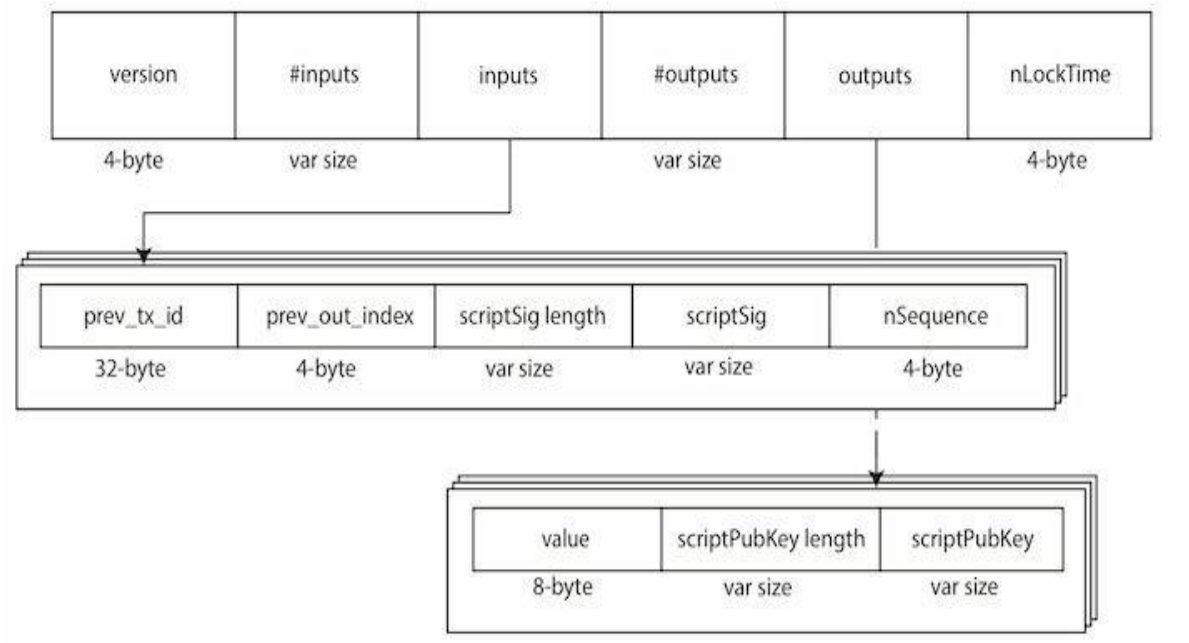
Conditions and Signatures: Bitcoin scripts can involve various conditions, such as requiring multiple signatures (multisig), time locks, or other custom rules. The scripts allow for flexible and programmable transactions.

Smart Contracts: While Bitcoin's scripting language is not as expressive as some other blockchain platforms, it can still be used to create simple smart contracts, enabling conditional payments and more complex transaction types.

Segregated Witness (SegWit): SegWit is a Bitcoin upgrade that changed the structure of transaction data and introduced witness data, which is a separate data structure that contains signatures. This upgrade aimed to improve network scalability and fix certain security issues.

Bitcoin's scripting language is intentionally limited to maintain security and prevent potential vulnerabilities, but it still provides a level of flexibility that enables a wide range of transaction types and use cases, making it more than just a simple peer-to-peer payment system.

USE CASES OF BITCOINBLOCKCHAIN SCRIPTING LANGUAGE IN MICROPAYMENT:



Bitcoin's scripting language can be used in various ways to facilitate micropayments, which are small transactions involving tiny amounts of value. Micropayments are especially valuable for content providers, online services, and digital goods, as they can enable more granular payment models. Here are some use cases of Bitcoin blockchain scripting language in micropayments:

Pay-per-View or Pay-per-Read Content: Content creators can use Bitcoin's scripting language to implement paywalls for their online articles, videos, or other digital content. Users would make small Bitcoin payments for access to individual pieces of content, making it economically viable for both content producers and consumers.

Microtransactions in Gaming: In online gaming, microtransactions are common for in-game items, power-ups, or customization options. Bitcoin scripting can be used to facilitate these microtransactions securely, allowing players to make small payments for virtual goods and services.

IoT and M2M Payments: The Internet of Things (IoT) devices often need to exchange small payments for data, services, or resources. Bitcoin scripting can be used to enable secure, automated micropayments between IoT devices, creating a more efficient and self-sustaining network.

Content Licensing: Artists and media creators can utilize Bitcoin scripting to implement automated licensing agreements for their work. Consumers can access and use content legally by making small, automatic payments each time they utilize it.

Adaptive Streaming Services: In media streaming, adaptive bitrate streaming adjusts the quality of video or audio in real-time based on the viewer's internet connection. Micropayments can be used to pay for content as it's consumed, ensuring fair compensation for the content provider.

In-App Purchases: Mobile apps and games can incorporate Bitcoin micropayments for in-app purchases. Users can buy virtual items, premium features, or ad-free experiences with small Bitcoin payments.

Online Tipping and Donations: Content creators, bloggers, streamers, and social media influencers can accept micropayments in Bitcoin from their audience as tips or donations.

This direct support can be more convenient and cost-effective than traditional payment methods.

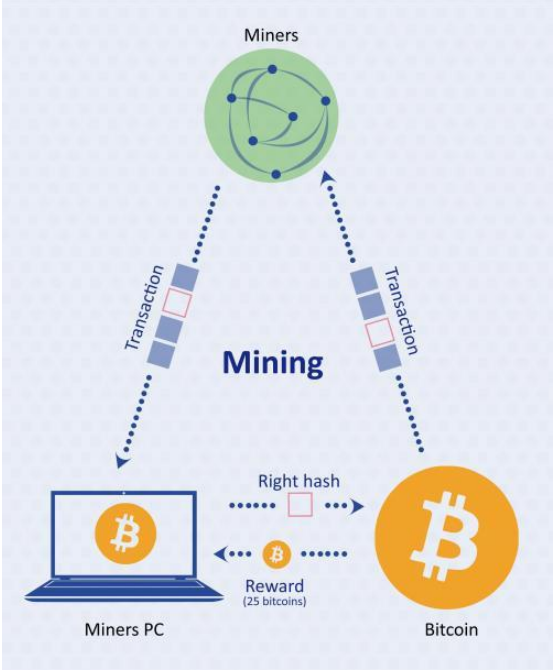
Microtransactions in Marketplaces: Online marketplaces can implement micropayments to facilitate the buying and selling of digital products, such as e-books, software plugins, stock photos, and more.

Pay-as-You-Go Services: Users can access various online services, like cloud storage or computing resources, on a pay-as-you-go basis, making small, automated payments with Bitcoin scripting.

Metered Utilities: Utility companies and service providers can use Bitcoin scripting for micropayments in metered services, such as electricity, water, or data usage. Users can pay only for what they consume.

Bitcoin's scripting language allows for the creation of versatile and flexible micropayment solutions. It offers advantages such as low transaction costs, security, and the ability to automate payments, making it a suitable choice for micropayments in various online and digital ecosystems. However, it's essential to consider scalability and potential network congestion when implementing such systems, as Bitcoin's blockchain has limitations in terms of transaction throughput.

ESCROW ETC DOWNSIDE OF BIT COIN MINING:



Bitcoin mining is a crucial component of the cryptocurrency's network, as it serves to secure transactions, validate blocks, and create new Bitcoins. While it has several advantages, there are also downsides and challenges associated with Bitcoin mining. Here are some of the downsides and concerns:

Energy Consumption: Bitcoin mining requires significant computational power, which translates to substantial energy consumption. As a result, Bitcoin mining can have a negative environmental impact, particularly when the electricity used is derived from non-renewable sources. This has raised concerns about the carbon footprint of the Bitcoin network.

Centralization: Over time, Bitcoin mining has become increasingly centralized due to the concentration of mining power in the hands of a few large mining pools and companies. This concentration can undermine the decentralization and security of the network, as it becomes more susceptible to attacks and manipulation by a single entity or a small group.

Hardware Costs: Mining Bitcoin effectively requires specialized hardware known as Application-Specific Integrated Circuits (ASICs). These devices are expensive and can quickly become obsolete as new, more efficient ASICs are developed. This can make it challenging for individual miners to stay competitive.

Competition: The Bitcoin network has a built-in mechanism that adjusts the difficulty of mining to ensure that new blocks are added roughly every 10 minutes. As more miners join the network, competition increases, making it harder for individual miners to earn rewards. This can lead to reduced profitability for small-scale miners.

Volatility: The value of mined Bitcoins is highly volatile, and miners may experience fluctuations in the value of their earnings. Market volatility can impact the profitability of mining operations, as Bitcoin's price can change rapidly.

Regulatory Uncertainty: Regulatory environments for cryptocurrency mining vary by country and can change over time. Some jurisdictions have imposed restrictions or banned mining activities, while others have embraced it. Regulatory uncertainty can create challenges for miners in terms of compliance and risk management.

Long Payback Period: Mining equipment is a significant upfront investment, and miners may not see a return on their investment for an extended period, especially if the price of Bitcoin drops or mining difficulty increases.

Security Risks: Bitcoin miners are exposed to risks associated with hardware failures, theft, and cyberattacks. The security of mining operations is critical to safeguard both the mining equipment and the mined Bitcoins.

Waste Heat: Mining hardware generates a substantial amount of heat, which can be challenging to manage effectively. Inefficient heat management can lead to increased cooling costs and environmental concerns.

Limited Anonymity: While Bitcoin is often touted as pseudonymous, miners' activities and earnings can be more easily traced and associated with their mining activities, potentially impacting their privacy.

It's important to note that while there are downsides to Bitcoin mining, there are also potential rewards, and many miners continue to participate in the network. The decision to mine Bitcoin depends on factors such as electricity costs, hardware investment, market conditions, and individual risk tolerance. As the cryptocurrency landscape evolves, these challenges may continue to be addressed and mitigated.

BLOCK CHAIN SCIENCE: GRID COIN, FOLDING COIN, BLOCK CHAIN GENOMICS, BIT COIN MOOC'S:

It seems like you've mentioned several concepts and projects related to blockchain technology and their applications in different fields.

Gridcoin: Gridcoin is a unique cryptocurrency that focuses on harnessing the computing power of distributed computing projects to contribute to scientific research, such as the search for extraterrestrial life and climate modeling. Gridcoin miners use their computing resources to perform these scientific computations, and in return, they receive Gridcoins as rewards. This concept is known as "Proof-of-Research" and is designed to reward individuals who contribute to scientific endeavors.

Gridcoin Crypto price in Indian rupees: (GRC – Grid Coin)

1 GRC = 0.86

5 GRC = 4.31 Rs

10 GRC = 8.62 Rs

50 GRC = 43.10 Rs

Foldingcoin: Foldingcoin is a digital token and another cryptocurrency project that encourages individuals to participate in scientific research. In this case, the project is specifically centered around protein folding simulations, a crucial aspect of understanding diseases like Alzheimer's and cancer. Participants contribute their computational power to run simulations that help scientists better understand protein folding, and they receive Foldingcoins as incentives.

What is Folding @Home?

- Folding @home (FAH) is a project by standford university that has been running since october 2000.
- FAH uses idle computer power to help simulate how proteins fold in the human body.
- This research is then used to help researchers find cures for diseases such as cancer and Alzhimers.

Blockchain Genomics: Blockchain technology is increasingly being explored in the field of genomics and healthcare. It can be used to securely and transparently manage genetic data, ensuring that patients have control over their genetic information and can share it with researchers or healthcare providers while maintaining privacy and security. It also offers the potential for incentivizing data sharing and collaboration.

A block chain is digital, decentralized public ledger designed to record every data on it’s network. Blockchain is widely deployed in various sectors, such as Finance, Education more.

- Block chain technology may be new, but it is already playing a major role in healthcare, especially in genomic medicine.

- As the technology becomes more widely used in genomics, scientists will be able to gain a deeper understanding of disease mechanisms.

- This knowledge will helps scientists develop better therapies and inventions for a variety of diseases while maintaining privacy and security.

Why Blockchain in Genomics???

- **Genomic Data Security:** Genomics data is very sensitive and crucial from a data security prespective, blockchain provides excellent data security and integrity. Security methods such as encryption are useful in combating data breaches, but they do not provide complete protection. Many systems How big are organizations with the high level of security and penetrated by hackers? However, blockchain technology helps organization by providing better protection against data breaches. Blockson uses hashing techniques to store data security, which helps the company in securing data and also helps in data sharing.

- **Genomic Data Sharing:** Using genomic data and the blockchain network. It is now. Possible to send anonymous genetic information around the world. The decentralization nature of blockchain allows easy and secure data exchange between the organizations. Information can be stored in special ledger in a blockchain database, keeps the information secured.

- **Immutability of Genomic Data:** Blocks in provides immutability of genomic data for organizations helping organizations protect information. Due to the decentralization structure of blocks and technologies, economic data cannot be modified. And so any changes will be reflected off on nodes so that no one cheats here. And it can be said that Genomic data sharing is very safe.

- **Cost Reduction:** Since blockchain does not require a 3rd person, it reduces cost for organizations and give trust to other partners as well. Before blockchain technology organizations spends lot of money as they have to hire their 3rd person to maintain all these things, which blocks and technology does.

Bitcoin MOOCs: MOOCs (Massive Open Online Courses) related to Bitcoin are educational resources that provide in-depth information about Bitcoin, its technology, and its applications. These courses cover topics like blockchain technology, cryptocurrencies, mining, and the broader economic and social implications of Bitcoin. They offer accessible ways for individuals to learn about Bitcoin and its ecosystem.

This Massive Open Online Course (MOOC) Is a basic introduction to Bitcoin. Its system network, protocol, blockchain, and digital currency for decision makers of enterprises, developers and students. The course covers the importance of bitcoins, urinal protocol provided by Santoshi Nakamoto, and how that original design is now used by Bitcoin SV. After this introductory course, you can opt to follow additional MOOCs To do a deep diving history, economy, development tooling and regulatory complaints associated with blockchain.

These concepts illustrate how blockchain technology can be applied to various fields beyond just finance. They demonstrate the potential for decentralized, secure, and transparent systems to contribute to scientific research, genomics, and education. Additionally, these projects highlight the innovative ways in which blockchain and cryptocurrencies can incentivize and reward participants in non-financial contexts.

THE END

THANK YOU

HAPPY LEARNING