BCT UNIT 2 - notes

Blockchain Technology (Jawaharlal Nehru Technological University, Hyderabad)

UNIT -II

Extensibility of Blockchain Technology Concepts

Extensibility refers to the ability of a system to adapt and evolve over time.

The extensibility of blockchain technology allows for the development of new use cases beyond its original intent. Extensibility is a critical factor in the ongoing success of blockchain technology.

Blockchain technology has a vast range of potential use cases, from supply chain management to identity verification to voting systems. The extensibility of blockchain technology allows for the creation of new use cases that were previously impossible. The potential use cases for blockchain technology continue to expand as the technology evolves.

It is necessary to understand the new ideas separately and together.

Blockchain Technology concepts include public-key and private-key cryptography, peer-to peer file sharing, distributed computing, network models, pseudonymity, blockchain ledgers, cryptocurrency protocols, and cryptocurrency.

It is a required to understand these concepts in order to operate in the blockchain technology environment. When you understand the concepts involved, it is not only possible to innovate blockchain-related solutions, but further, the concepts are portable to other contexts

This extensibility of blockchain-related concepts may be the source of the greatest impact of blockchain technology as human agents understand these concepts and deploy them in every venue they can imagine

One broad way of thinking about the use of blockchain concepts is applying them beyond the original context. The extensibility of blockchain technology allows for the creation of new use cases and the evolution of existing one

However, there are significant challenges to be addressed, including scalability, privacy, governance, and sustainability.

As blockchain technology continues to evolve, its potential use cases will continue to expand.

Some of the challenges to be addressed are:

Smart Contracts

Interoperability

Scalability

Privacy

Governance

Sustainability

Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code.

Smart contracts are a key innovation in blockchain technology, enabling the automation of complex processes.

Smart contracts have the potential to transform many industries, including financial services, real estate, and supply chain management.

Scalability

Scalability refers to the ability of a system to handle increasing amounts of work without impacting performance

Scalability is a significant challenge for blockchain technology, which currently struggles with slow transaction processing and high fees.

Several solutions are being developed to address scalability, including sharding, layer 2 solutions, and blockchain interoperability.

Interoperability

Interoperability refers to the ability of different blockchain networks to communicate and work together seamlessly.

Interoperability is critical for the widespread adoption of blockchain technology.

Several projects are underway to develop interoperability solutions, including Polkadot, Cosmos, and Ark.

Privacy

Privacy is a critical concern for many blockchain use cases, particularly those involving sensitive data.

Several privacy-focused blockchain projects, such as Monero and Zcash, have emerged to address this issue.

Privacy-enhancing technologies, such as zero-knowledge proofs, are also being developed to improve privacy on public blockchains.

Governance

Governance refers to the systems and processes in place to manage and regulate a blockchain network.

Effective governance is essential for the ongoing success of blockchain projects.

Several governance models exist, including on-chain governance, off-chain governance, and hybrid models.

Sustainability:

Sustainability refers to the ability of a blockchain network to operate over the long term.

Blockchain networks require significant computing power and energy consumption, which can be a barrier to sustainability.

Several projects are exploring alternative consensus mechanisms, such as proof of stake, to improve sustainability.

Some of the use cases of Blockchain are:

Financial Services

Supply chain Management

Health Care

Identity Management

Voting Systems

Financial Services

Blockchain technology has the potential to transform the financial services industry by enabling faster, more secure, and more efficient transactions.

Use cases for blockchain in financial services include cross-border payments, trade finance, and digital identity.

Several blockchain projects are focused on financial services, including Ripple, Stellar, and Corda.

Supply Chain Management

Blockchain technology can improve supply chain management by increasing transparency and traceability, reducing fraud and counterfeiting, and improving efficiency.

Use cases for blockchain in supply chain management include tracking the origin and movement of goods, verifying product authenticity, and reducing waste.

Several blockchain projects are focused on supply chain management, including VeChain, Waltonchain, and Ambrosus.

Healthcare

Blockchain technology has the potential to transform the healthcare industry by improving patient data management, reducing fraud, and increasing transparency.

Use cases for blockchain in healthcare include patient data management, clinical trials, and drug supply chain management.

Several blockchain projects are focused on healthcare, including MedRec, Medicalchain, and FarmaTrust.

Identity Management

Blockchain technology can improve identity management by reducing fraud, increasing security, and improving privacy.

Use cases for blockchain in identity management include digital identity, KYC/AML compliance, and secure authentication.

Several blockchain projects are focused on identity management, including Civic, uPort, and SelfKey.

Voting Systems

Blockchain technology can improve voting systems by increasing transparency, reducing fraud, and improving accuracy.

Use cases for blockchain in voting systems include online voting, secure and anonymous voting, and election auditing.

Several blockchain projects are focused on voting systems, including Follow My Vote, Agora, and Horizon State.

Digital identity verification in blockchain

Digital identity verification in blockchain refers to the process of securely and reliably verifying the identity of individuals or entities in a digital environment using blockchain technology. Traditional identity verification methods often rely on centralized databases and third-party intermediaries, which can lead to issues related to privacy, security, and control over personal data. Blockchain offers a potential solution by providing a decentralized and transparent way to manage digital identities.

Here's how digital identity verification can work in a blockchain context:

Decentralized Identity: In a blockchain-based digital identity system, individuals can have control over their own digital identities. Instead of relying on a central authority to validate and store identity data, users maintain ownership of their personal information and can choose when and with whom to share it.

Self-Sovereign Identity (SSI): Self-sovereign identity is a concept where individuals have complete control over their identity data and can share it with others on a need-to-know basis. Blockchain provides the technology to implement SSI by allowing users to create and manage their identities through cryptographic keys.

Identity Attributes: Instead of sharing entire identity profiles, individuals can share specific attributes (like age, address, or certification) when needed. These attributes are stored on the blockchain and can be verified by cryptographic proofs without revealing the underlying data.

Blockchain Immutability: Once identity attributes are recorded on a blockchain, they are tamper-proof and cannot be altered without consensus from the network. This enhances the security and integrity of identity data.

Private and Public Keys: Users have a private key that they use to sign transactions and prove ownership of their identity attributes. The corresponding public key can be used by others to verify the authenticity of the provided data.

Decentralized Consensus: Blockchain's consensus mechanisms ensure that identity attributes are verified by multiple participants in the network, reducing the risk of fraudulent or incorrect information.

Interoperability: Blockchain-based identity systems can potentially enable cross-platform and cross-border verification without the need for intermediaries. This can be particularly useful in scenarios like international travel or online service access.

Use Cases: Digital identity verification in blockchain has applications in various domains, including financial services, healthcare, supply chain management, voting systems, and more.

It's important to note that while the concept of blockchain-based digital identity holds promise, there are also challenges to address, including user adoption, standardization, scalability, and potential risks related to the storage of private keys. Additionally, regulations and legal frameworks need to be considered to ensure that these systems meet legal requirements and provide adequate protection to users.

Cryptography experts and blockchain developers and architects point out the importance of designing the blockchain industry with some of the same principles that have become baked into the Internet structure over time, like neutrality.

In the case of the Internet, net neutrality is the principle that Internet service providers should enable access to all content and applications regardless of the source and without favoring or blocking particular products or websites.

Blockchain Neutrality:

The concept is similar for cryptocurrencies.

Bitcoin neutrality means the ability for all persons everywhere to be able to easily adopt Bitcoin. This means that anyone can start using Bitcoin, in any and every culture, language, religion, and geography, political system, and economic regime.

For example, the Islamic Bank of Bitcoin is investigating ways to conduct Sharia-compliant banking with Bitcoin.

A key point of Bitcoin neutrality is that the real target market for whom Bitcoin could be most useful is the “unbanked,” individuals who do not have access to traditional banking services for any number of reasons, estimated at 53 percent of the worldwide population.

Bitcoin neutrality means access for the unbanked and underbanked, which requires Bitcoin solutions that apply in all low-tech environments, with features like SMS payment, paper wallets, and batched blockchain transactions.

Having neutrality-oriented, easy-to-use solutions for Bitcoin could trigger extremely fast uptake in underbanked markets.

There are different SMS Bitcoin wallets and delivery mechanisms (like

37Coins[96] and Coinapult, and projects like Kipochi[97] that are integrated with commonly used emerging-markets mobile finance platforms like M-Pesa.

Digital Divide of Bitcoin

The term digital divide has typically referred to the gap between those who have access to certain technologies and those who do not. In the case of cryptocurrencies, if they are applied with the principles of neutrality, everyone worldwide might start to have access. Thus, alternative currencies could be a helpful tool for bridging the digital divide.

However, there is another tier of digital divide beyond access: know-how. A new digital divide could arise (and arguably already has in some sense) between those who know how to operate securely on the Internet and those who do not. The principles of neutrality should be extended such that appropriate mainstream tools make it possible for anyone to operate anonymously (or rather pseudonymously), privately, and securely in all of their web-based interactions and transactions.