Date

BLOCKCHAIN TECHNOLOGY - UNIT-3

• CRYPTOCURRENCIES AND DIGITAL ASSETS

- A cryptocurrency is a digital form of currency that uses cryptography and blockchain to secure transactions, control creation of new units, and validate ownership.
- Cryptocurrencies are decentralized, borderless and trustless.

Characteristics

- Based on BT
- Secured using public-private key cryptography
- transparent & immutable
- Irreversible transactions
- Decentralized & peer to peer
- limited supply
- Global and borderless

Examples: Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Ripple (XRP)

Role of Blockchain in cryptocurrencies

- distributed ledger for transaction history
- security through cryptographic hashing
- consensus mechanism (PoW, PoS) for validation
- Pseudonymity via public key addresses.
- Traceability via audit trials
- Protection from double spending

Spiral

Date

Digital Assets

- any item that exists in digital form and has ownership or economic value.
- blockchain converts such assets into unique, verifiable and tradable tokens.
- Example : Cryptocurrencies, Utility tokens, Security tokens, NFTs, Stablecoins.

Tokenization

- process of converting real world assets into digital tokens on blockchain.
- The assets can be physical (land, art), financial (stocks, bonds) or intangible (intellectual property).
- divisible ownership
- 24/7 trading
- transparent tracking
- Global liquidity
- Reduced intermediaries
- Automated compilance - check

NFTs (Non Fungible Tokens)

- It represents unique digital assets stored on blockchain.
- Each NFT has distinct identity and metadata, making it non-interchangeable.
- Example : Digital art, Music, Videos, Game items, etc.

Stablecoins

- cryptocurrencies pegged to stable assets such as fiat currencies (USD) or commodities (gold). USDT, USDC

Spiral

Date

• SUPPLY CHAIN MANAGEMENT

- Supply chain management involves the movement of goods, information, and finances from suppliers to manufacturers, distributers, retailers and final consumers.
- Traditional supply chains lack transparency, allow fake products, depend on slow paperwork, risk data manipulation, and make product tracking difficult.

Functional Working

1. A product is manufactured and assigned a unique digital identity (token/QR/NFC tag)
2. Each supply chain event (storage, transport, inspection) is recorded on blockchain (cloudbased storage)
3. IoT devices track temp, location and shipment status in rt.
4. Smart contracts automate payments, customs checks, and authorization
5. Consumer or regulators can verify product origin and authenticity at any time. (AI and analytics)

Benifits

- Transparency & Traceability
- Anti-counterfeiting (No fake)
- cost and time efficient
- Better compilance & auditability
- Enhanced consumer trust.

Role of Blockchain

- End to end transparency
- Immutability
- Real time tracking of goods
- Smart contracts for automation

Spiral

Date

- Provenance tracking for authenticity and quality assurance.
- Efficient recall mechanisms in case of defective batches
- Example: Walmart & IBM food trust, De Beers, Pharmaceutical supply chains, FedEx & DHL (shipment tracking)

IDENTITY MANAGEMENT

- It refers to the process of verifying, storing and managing an individual's or entity's information such as name, age, nationality, etc
- Traditional identity systems depends on centralised authorities like govt, banks and institutions.
- These systems are vulnerable to data breaches and identity theft, reduce user privacy, provide limited user control, and make cross border identity verification slow & inefficient.

Blockchain based identity Management

1. Decentralized Identifiers (DIDs) - unique, verifiable digital identifier
2. verified credentials - docs can be cryptographically verified
3. Self Sovereign Identity (SSI) - individuals own and manage their identities.
4. Zero Knowledge Proofs (ZKPs) - prove certain facts without revealing full identity info.

Spiral

Date

Process

1. User creates a DID and a key pair
2. Identity credentials (passwords, KYC data) are issued by trusted authorities and linked to the DID.
3. When required, user proves identity via cryptography or ZKP.
4. Smart contracts verify validity without storing actual data on chain
5. Access are granted only when conditions are met.

Benifits

- Enhanced security
- User control & privacy
- Reduced fraud
- Efficient onboarding
- Global interoperability

Example: uPort, Civic, Sovrin Network, Microsoft ION

- **HEALTH CARE & MEDICAL RECORDS**

- Traditional healthcare systems rely heavily on centralized databases, paper documentation, and manual verification processes, making them vulnerable to tampering, loss, duplication and unauthorized access.
- fragmented health data, poor interoperability, manual insurance, prescription errors, lack of transparency.

Spiral

Date

Working

1. A person undergoes diagnosis or treatment
2. Medical record is generated and hashed
3. Record is time stamped and stored securely on blockchain
4. Patient hold private key and controls who can view the data
5. Hospitals/pharmacies can access the data only with user permission
6. Smart contracts automate prescription verification, insurance claims, and data sharing.
7. All changes are logged immutably for auditing and legal use.

Benifits of BT in Healthcare

- Patient's centric Record Ownership
- Interoperability Across systems
- Prevention of data tampering
- Improved diagnosis and Treatment
- Insurance automation - smart contracts
- secure sharing of sensitive data - ZKPs
- Medical Research & Analysis

Example:
MedRec
PharmaLedger
BurstIQ
MedicalChain

Use of Smart contracts

- Insurance claim approval
- Prescription authentication
- Appointment scheduling & billing
- Consent management
- Clinical trial data management

Integration with IoT & AI

- Predictive diagnosis
- Personalised treatments
- continous patient monitoring
- automated alerts for abnormalities

Spiral

2. Privacy and Security in Blockchain

a) Privacy-enhancing Techniques

Privacy is vital in sensitive areas like finance or healthcare.

1. **Ring Signatures**:
   - Conceals the sender's identity by combining it with a group of other possible senders.
   - All members in the group sign the transaction, making it impossible to identify the real sender.
   - **Example**: **Monero**, a privacy-focused cryptocurrency, uses ring signatures.
2. **Zero-Knowledge Proofs (ZKPs)**:
   - Prove that you know something (e.g., a password) without revealing the actual information.
   - **Example**: **ZCash** uses zk-SNARKs for private cryptocurrency transactions.

Technical Insight: In ZKP, if Alice wants to prove to Bob she knows the password to a vault:

- Alice performs a mathematical computation (proof).
- Bob verifies the computation without ever learning the password.

---

b) Security Vulnerabilities and Attacks

1. **51% Attack**:
   - If a group controls over 50% of blockchain's computational power, they can:
     - Rewrite parts of the blockchain.
     - Reverse transactions (double-spending).
   - **Example**: In 2019, Ethereum Classic suffered a 51% attack, leading to losses of millions.
2. **Smart Contract Exploits**:
   - Vulnerabilities in smart contracts can result in exploits.
   - **Example**: The DAO hack on Ethereum in 2016 caused a loss of $50 million due to a loophole in the smart contract.

---

c) Auditing and Accountability

Blockchain's **immutable nature** makes it ideal for auditing:

- Transactions cannot be altered or deleted.
- Each action is permanently recorded.

Example:

- **Chainalysis**: Helps governments and businesses audit blockchain transactions to ensure compliance with regulations.
