U-1 (BT)

DOMS | Page No.
Date / /

Blockchain →

advanced database mechanism that allows transparent information sharing within business network

- stores data in blocks that are linked together in a chain.
- Imp concepts
  - Blocks → Data in block
  - Node → Branches
  - Miner → create new blocks on chain through process → mining.

Blockchain Appln

- Cryptocurrency
- Cybersecurity
- Accounting & record keeping
- Supply Chain
- Healthcare
- Automobile
- Govt.
- Sports.
- E-commerce.

DOMS | Page No.
Date / /

Symmetric key cryptography

- encryption & decryption use same key for both ends of conversation.
- cipher text → same or smaller (than original)
- encryption is fast
- transfer large data.
- provides confidentiality
- key length → 128 or 256 bits
- resource utilization is less
- security is less as one key for 2 purpose.
- Isn't used in digital signatures.

Asymmetric

- Two diff keys - public key & private key
- cipher text → same or larger (original)
- slow
- transfer small amt of data
- provides confidentiality, authenticity & non-repudation
- 2048 or higher
- resource utilization is high
- more secure.
- Is used in digital signatures.

DOMS | Page No.
Date / /

Elliptic Curve Cryptograph (ECC)-

- key based technique for encrypting data.
- focuses on pairs of public & private keys for decryption & encryption.
- substitute for RSA cryptographic algo.
- Decryption take more time.
- Much safer than RSA & is currently in process of adapting.
- encryption takes less time.
- relies on properties of elliptic curves,

$$y^2 = y^3 + ax + b.$$

(x, y)

curves have set of points that satisfy eqn.

- public key is derived from private key
- ECC → used for digital signatures.

Use Cases → used in secure communication protocols
- SSL/TLS for secure web browsing

DOMS | Page No.
Date / /

Cryptographic Hash functions-

- cryptographic tool → transform input data into fixed-size string of characters.
- verify data integrity & create digital signatures
- unique hash → each unique input.
- small change in input → vastly different hash.
- Hash → irreversible.
- Popular hash algo → SHA-256 & MD5.
- used to password storage to protect user data.
- resistent to collision. (same hash for diff inputs)
- Data verification
- data security / integrity

DOMS | Page No.
Date / /

SHA (256) - Secure Hash Algo.

- Message length
- Digest length
- Irreversible

- cryptographic hash function.
- data integrity & security.
- input data & produces 256 fixed size hash value.
- Is irreversible, can't deduce input from hash.
- change in input → diff hash.
- verify data integrity.
- part of SHA-2 family.
- password storage & digital signature.
- quick & reliable way to verify data.
- Used in cryptocurrency → Bitcoin
- crucial for ensuring security & trustworthiness

DSA - Digital Signature Algo

- assymteric cryptographic algo
- For digital signature.
- involves pair of public & private key
- signature → prove authenticity of msg

Benefits → Message Authentication
→ Integrity verification
→ Non-repudiation

- Highly robust
- Better speed
- Less storage
- Patent Free

Steps → Key Generation
Signature "_"
Key Distribution
Signature Verfic"

DOMS | Page No.
Date / /

Merkle Tree -

- fundamental part of BCT
- ds → data verification.
- integrity & validity of data.
- saving memory or disk space
- proofs & management require → tiny amt of info → transmit across network
- organize data in bisocial tree like structure
- each leaf → piece of data or transaction.
- Parent node → hashes of child node.
- top node → root → represents entire dataset.
- verify specify data → within a large dataset.
- reduce need to process all data for verification

Benefits of Blockchain.

- Security & Immutable Records
- Reduced Fraud & Chargebacks.
- Decentralized.
- Faster Transactions.
- Lower Transaction cost
- Improved Transparency
- Cross-Border Payment
- Data Privacy

Limitation of BCT

- Data Recovery
- Adoption & Education
- Integration Challenge
- energy consumption.
- scalability →
- latency
- Transaction costs
- User Experience
- Regulatory Compliance
- Lack of Regulation.

	Centralization	Decentralization
Third Party involve	Yes	No
Control	Full control with central authority	Control with users
Hackable	More prone	Less prone.
single point of failure	Yes	No.
Ease of use	Easy	Not easy.
exchange fees	Higher fees	Less Fees.
Anonymous	User Not anonymous	offers anonymity.
Decision making	Slow	Fast
Communn flow	systemized vertically	Free & open
Prime benefit	Proper leadership & coordination	Sharing responsibilities & workload
Appln	small sized organization	large sized organization

DOMS | Page No.
Date / /

Blockchain Layers:

1) Appln & Presentation Layer • top layer of BT
   - user interface & appln built.
   - wallet management, smart contract execution
   - directly interact with various BC activities.
   - bridge technical complexity of blockchain for end user.
   - adopn & usability.

2) Data Layer-
   - blockchains data structure resides.
   - chain of blocks → set of transactions
   - data storage & retrieval mechanism.
   - distributed database

3) Network Layer:
   - handles communicn & connectivity aspects of network
   - peer to peer connection b/w nodes.
   - exchange info
   - Bitcoin Network protocol

4) Conserss Layer -
   - all nodes on network agree on state of blockchain
   - rules & mechanisms for validating & adding new transaction
   - prevents double spending & secures blockchain agnst malicious actors.

5) Infrastruc or hardware Layer
   - ↳ involves deployment & maagmet of nodes or servers
   - ↳ highly specialized & engery intensive
   - ↳ data center provides necessary infrastructure
   - ↳ high speed internet → crucial for nodes.
   - ↳ security considerations are critical.