Maulana Azad National Urdu University

M.Tech. II Semester Examination, July 2023

Paper - MTCS231PET : Blockchain Technology

پرچہ : بلاک چین ٹکنالوجی

Time : 3 hrs **Marks : 70**

ہدایات:ہدایات:

یہ پرچہ سوالات تین حصوں پر مشتمل ہے: حصہ اول، حصہ دوم، حصہ سوم۔ ہر جواب کے لئے لفظوں کی تعداد اشارۃً ہے۔ تمام حصوں سے سوالوں کا جواب دینا لازمی ہے۔

1. **حصہ اول** میں 10 لازمی سوالات ہیں جو کہ معروضی سوالات/ خالی جگہ پُر کرنا/مختصر جواب والے سوالات ہیں۔ ہر سوال کا جواب لازمی ہے۔ ہر سوال کے لیے 1 نمبر مختص ہے۔ **(10 x 1 = 10 Marks)**
2. حصہ دوم میں آٹھ سوالات ہیں۔اس میں سے طالب علم کو کوئی پانچ سوالوں کے جواب دینے ہیں۔ ہر سوال کا جواب تقریباً دوسو(200)لفظوں پر مشتمل ہے۔ ہر سوال کے لیے 6 نمبرات مختص ہیں۔ **(5 x 6 = 30 Marks)**
3. حصہ سوم میں پانچ سوالات ہیں۔اس میں سے طالب علم کو کوئی تین سوالوں کے جوب دینے ہیں۔ ہر سوال کا جواب تقریباً پانچ سو(500)لفظوں پر مشتمل ہے۔ ہر سوال کے لیے 10 نمبرات مختص ہیں۔ **(3 x 10 = 30 Marks)**

حصہ اول

سوال:1

i. ..... Message کو محفوظ بنانے کے لیے تبدیل کرنے کا سائنس (Science) اور فن (Art) ہے

(a) Cryptography (b) Calligraphy (c) Cryptoanalysis (d) ان میں سے کوئی نہیں

ii. SHA - 256 Algorithm میں Round Computation کے مراحل کی تعداد کیا ہے؟

(a) 80 (b) 76 (c) 64 (d) 70

iii. ..... لفظ (Term) کا استعمال Blockchain Splits کے لیے کیا جاتا ہے؟

(a) A Merger (b) A Fork (c) A Division (d) ان میں سے کوئی نہیں

iv. Blockchain میں ..... tree، کسی Block کے تمام Transactions کے (Digital Fingerprints) کو محفوظ رکھتا ہے

(a) Merkle (b) Binary (c) AVL (d) Red Black

v. DAPP کیا ہے؟

(a) A blockchain network (b) Type of Cryptocurrency

(c) Hardware Component (d) Decentralized Application

vi. Blockchain کے First Block کا نام کیا ہے؟

(a) Genesis Block (b) Origin Block (c) Block one (d) ان میں سے کوئی نہیں

vii. Miners کے Transaction Validate کرنے پر کیا Incentive ملتا ہے؟

(a) Appreciation of the community (b) Nance

(c) Block Rewards (d) Additional Memory

viii. Blockchain بنانے کا مطلوبہ مقصد (Intended Objective) کیا تھا؟

Research Project (a)
Peer-to-peer Electronic Cash System (b)
Open-source Network for Connecting Banks (c)
ان میں سے کوئی نہیں (d)

ix. Hyperledger Fabric میں طے شدہ Ledger System کے لیے کس Database کا استعمال کیا جاتا ہے؟

MySQL (a)
Couch DB (b)
MS-SQL (c)
Level DB (d)

x. Transactions کو Endorse کرنے کے لیے آپ کو کتنے Peers کی ضرورت ہوتی ہے؟

10 (a)
03 (b)
05(c)
Depends on Endorsement Policy (d)

حصہ دوم

2- SHA-256 کو کسی خاکہ (Diagram) کی مدد سے تفصیل سے بیان کریں۔

3- Fork کیا ہے؟ Fork کے اقسام پر بحث کریں۔

4- Proof-of-Stake پروٹوکول کی خاکہ کی مدد سے وضاحت کریں۔

5- Web 1.0, Web 2.0 اور Web 3.0 کے درمیان فرق لکھیں۔

6- Endorsing Peer اور Committing Peers کے درمیان فرق لکھیں۔

7- Deterministic اور Non-Deterministic کی مثال کے ساتھ وضاحت کریں۔

8- Fabric Blockchain Network میں Transaction کیسے شامل ہوتا ہے؟

9- Ethereum Network پر Robin نے Bob 20 Ethers کو بھیجتا ہے۔ Gas کی Gas Limit 21000 ہے۔ Gas کی قیمت 100 gwei گیس ہے اور 5 gwei priority fees گیس ہیں ، Transaction میں Ethers کی Fees کا حساب (Calculate) کریں۔

حصہ سوم

10- Plaintext کے ایک Block کو ElGamal Encryption کا استعمال کرتے ہوئے Encrypt کیا گیا ہے۔ فرض کریں کہ:

Prime number (p) = 11,

اور Primitive Root (e_1) = 2,

ہے recipient private key (d) = 3

جب $C_2 = 6$ اور $C_1 = 5$ ہو تب Ciphertext سے مطابقت (Corresponding) رکھنے والا Plaintext کیا ہے

11- درج ذیل پر مختصر نوٹ لکھیے۔

Double Spending Money (a)
Uncle Block (b)
Stale Block (c)
Orphand Block (d)

12- Proof-of-work (PoW) Consensus Algorithm کا استعمال کرتے ہوئے Bitcoin Network کے Mining کے عمل کی وضاحت کریں۔

13 Smart Contract کی خصوصیات لکھیں۔ Solidity میں Variables ، Variable Scope اور Data Types کی وضاحت کریں

14- Diagram کی مدد سے Hyperledger کے Transaction Flow کے عمل کی وضاحت کریں۔

☆☆☆