Maulana Azad National Urdu University

Ph.D. (Computer Science) Coursework I Semester Examination, December 2023

بلاک چین ٹیکنالوجی

PHCS118DST: Block chain Technology

Time : 3 hrs **Marks : 70**

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 جواب 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 نمبر : 1

i. input میں کی جانے والی بھی تبدیلی (change)، چاہے وہ کتنی چھوٹی ہو اس کے نتیجے میں output hash میں بڑی تبدیلی آئے گی جسے _____ کہا جاتا ہے۔

Determinism (d) Avalanche effect (c) non- repudiation (b) Collision (a)

ii. _____ algorithm جو key arrangement اور exchange کے problem پر قابو پانے کے لیے استعمال کیا جاتا ہے۔

iii. _____ valid blocks ہیں جو blockchain میں شامل کرنے کے لیے درکار تمام ضروری requirments کو پورا کرتے ہیں، لیکن پھر بھی rejected کر دیئے جاتے ہے۔

Uncle (d) Stale (c) Orphan (b) Genesis (a)

iv. Distributed Ledger Technologies یا Blockchain کے پیشرو (predecessors) ہیں۔

False(b) True(a)

v. Ethereum _____ کا سب سے چھوٹا denomination ہے۔

Bitcoin (d) Ether (c) Wei (b) Gwei (a)

vi. Bitcoin network میں unconfirmed transactions کے لیے _____ ایک temporary storage ہے۔

Miner (d) Merkle Tree (c) Nonce (b) Mempool (a)

viii. _____ Hyperledger کا استعمال web3 application کو بنانے اور scale کرنے کے لیے کیا جاتا ہے۔

Bevel (d) Besu (c) Firefly (b) Cacti (a)

P.T.O.

viii. blockchain کا _____ ایک storevalue-keyversioned کے طور پر بنایا گیا ہے۔

(a) Node (b) Ledger (c) Block (d) Bevel

ix. identity اور attributesassociated کے union کو _____ کہا جاتا ہے۔

(a) PDC (b) MSP (c) Principal (d) Channel

x. اس activity کی شناخت کریں، جو lifecyclechaincode کا حصہ نہیں ہے۔

(a) Package (b) Install (c) Approve (d) None of the above

حصہ دوم

2. public parameters p=3, q=11 کے ساتھ two parties کے درمیان message M=10 کو communicate کرنے کے لیے RSA asymmetric cryptography میں شامل encryption اور decryption کے steps کا مظاہرہ کریں۔

3. Block chain میں UTXO کیا ہے؟ وضاحت کریں کہ یہ double-spending کو کیسے prevent کرتا ہے۔

4. PoW اور PoS کی وضاحت کریں اور ان کے درمیان فرق کو نمایاں کریں۔

5. Hyperledger Fabric کے block structure پر بحث کریں۔

6. Hyperledger Fabric میں Data Distribution Protocol کی وضاحت کریں۔ یہ consistency اور integrity کو یقینی بنانے کے لیے کس طرح مدد فراہم کرتا ہے؟

7. private data collection کیا ہے؟ network میں اس کے استعمال کا مظاہرہ کریں۔

8. Transaction کو endorse کرنے کے لیے آپ کو کتنے peers کی ضرورت ہے؟ Endorsement policies پر تبادلہ خیال کریں۔

9. chaincode lifecycle کے stages کی وضاحت کریں۔

حصہ دوم

10. ElGamalAsymmetric cryptosystem کے steps لکھیں۔ parameters p=11, g=2 کے ساتھ دو parties کے درمیان Mmessage 10= کو communicate کرنے کے لیے Elgamal encryption میں شامل steps کا مظاہرہ کریں۔ blockchain میں Zero-Knowledge Proof کا کیا کردار ہے؟

11. درج ذیل پر تفصیل سے بحث کریں:

a. Merkle Tree b. Fork c. Orphaned Block

d. Stale Block e. Uncle Block

12. Miners کے role کی وضاحت کریں اور mempool سے transaction کے selecting اور committing کے criteria پر تبادلہ خیال کریں۔ blockchain میں EVM کیسے کام کرتی ہے؟

13. Hyperledger Fabric کا architecture بنائیں اور Hyperledger Fabric کے transaction life-cycle کی وضاحت کریں۔

14. RAFT Consensus algorithm کے steps کو diagram کی مدد سے تفصیل سے بیان کریں۔

☆☆☆