Foundation of Blockchain (4361603) - Winter 2024 Solution

Milav Dabgar

November 25, 2024

પ્રશ્ન 1(a) [3 ગુણ]

Short Note on: Distributed Ledger

જવાબ

જવાબ:

કોષ્ટક 1. Distributed Ledger Features

પાસું	વર્ણન
વ્યાખ્યા	ડેટાબેઝ જે અનેક કોમ્પ્યુટર્સ પર ફેલાયેલો છે
સંગ્રહ	ડેટા અનેક સ્થાનો પર સંગ્રહિત થાય છે
નિયંત્રણ	કોઈ એક સત્તાધિકારી તેની માલિકી ધરાવતું નથી
અપડેટ્સ	બધા નકલો એક સાથે અપડેટ થાય છે

- **વિકેન્દ્રીકૃત**: કોઈ કેન્દ્રીય સર્વરની જરૂર નથી
- **પારદર્શક**: બધા સહભાગીઓ વ્યવહારો જોઈ શકે છે
- **સુરક્ષિત**: સુરક્ષા માટે ક્રિપ્ટોગ્રાફીનો ઉપયોગ કરે છે

મેમરી ટ્રીક

ડેટા સંગ્રહિત પારદર્શક રીતે સુરક્ષિત (DSTS)

પ્રશ્ન 1(b) [4 ગુણ]

Describe the applications of Blockchain.

જવાબ

જવાબ:

કોષ્ટક 2. Blockchain Applications

એપ્લિકેશન	ઉપયોગ	ફાયદો
Cryptocurrency	Bitcoin જેવું ડિજિટલ નાણું	સુરક્ષિત ચૂકવણી
Supply Chain	સ્ત્રોતથી પ્રોડક્ટ્સ ટ્રેક કરવા	નકલી માલ અટકાવવા
Healthcare	મેડિકલ રેકોર્ડ્સ સંગ્રહવા	ડેટા સુરક્ષા
Voting	ઇલેક્ટ્રોનિક વોટિંગ સિસ્ટમ	પારદર્શક ચૂંટણીઓ
Real Estate	મિલકત રેકોર્ડ્સ	છેતરપિંડી અટકાવવા

- **Finance**: ઝડપી આંતરરાષ્ટ્રીય ચૂકવણી
- **Identity**: ડિજિટલ ID ચકાસણી
- **Smart Contracts**: સ્વચાલિત કરારો

મેમરી ટ્રીક

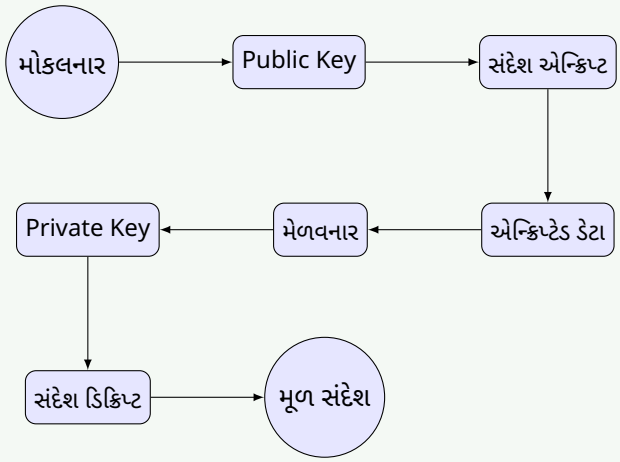
પૈસા, દવા, મતદાન, મિલકત (MMVP)

પ્રશ્ન 1(c) [7 ગુણ]

Explain Asymmetric Encryption Model with example.

જવાબ

જવાબ:
Asymmetric Encryption Process



આકૃતિ 1. Asymmetric Encryption પ્રક્રિયા

કોષ્ટક 3. Key તફાવત

Key પ્રકાર	હેતુ	શેરિંગ	ઉદાહરણ
Public Key	Encryption	ખુલ્લેઆમ શેર થાય છે	RSA Public Key
Private Key	Decryption	ગુપ્ત રાખવામાં આવે છે	RSA Private Key

ઉદાહરણ પ્રક્રિયા:
1. Alice Bob ને સંદેશ મોકલવા માંગે છે
2. Alice Bob ની public key વાપરીને encrypt કરે છે
3. ફક્ત Bob ની private key decrypt કરી શકે છે
4. Bob સંદેશ મેળવે છે અને decrypt કરે છે

- **સુરક્ષા**: Public key જાણીતી હોવા છતાં ડેટા સુરક્ષિત રહે છે
- **પ્રમાણીકરણ**: મોકલનારની ઓળખ સાબિત કરે છે
- **Non-repudiation**: મોકલનાર મોકલવાનો ઇનકાર કરી શકતો નથી

મેમરી ટ્રીક

જાહેર એન્ક્રિપ્ટ, ખાનગી ડિક્રિપ્ટ (PEPD)

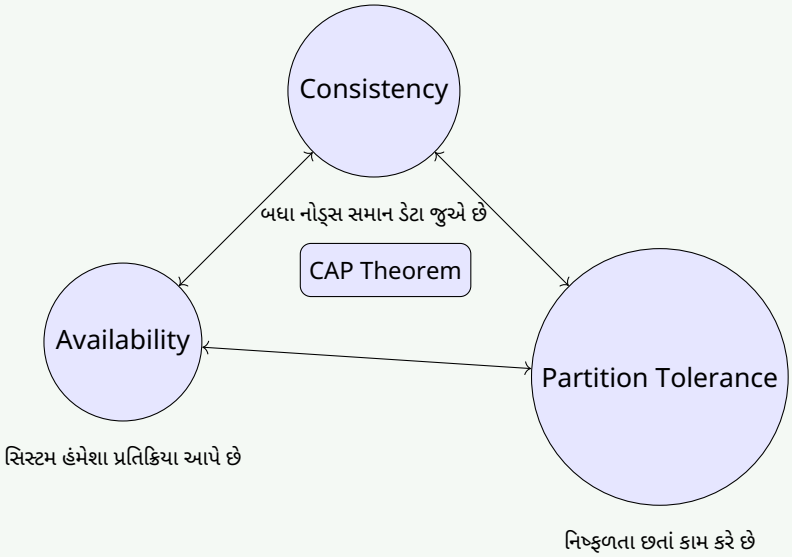
OR

પ્રશ્ન 1(c) [7 ગુણ]

Explain Consistency, Availability and Partition Tolerance (CAP) theorem in Blockchain.

જવાબ

જવાબ:
CAP Theorem ત્રિકોણ



આકૃતિ 2. CAP Theorem ગુણધર્મો

કોષ્ટક 4. CAP ગુણધર્મો

ગુણધર્મ	વ્યાખ્યા	Blockchain ફોકસ
Consistency	બધા નોડ્સ પાસે સમાન ડેટા હોય છે	મધ્યમ અગ્રતા
Availability	સિસ્ટમ હંમેશા પ્રતિક્રિયા આપે છે	ઉચ્ચ અગ્રતા
Partition Tolerance	નેટવર્ક વિભાજન છતાં કામ કરે છે	ઉચ્ચ અગ્રતા

મુખ્ય મુદ્દાઓ:
- **Trade-off**: 3 માંથી માત્ર 2 ગુણધર્મો પૂરા કરી શકાય
- **Blockchain પસંદગી**: સામાન્ય રીતે Availability + Partition Tolerance પસંદ કરે છે
- **વાસ્તવિક ઉદાહરણ**: Bitcoin C કરતાં AP પસંદ કરે છે (eventual consistency)

મેમરી ટ્રીક

કોઈપણ બે પસંદ કરો (CAT)

પ્રશ્ન 2(a) [3 ગુણ]

Define: Public key, Private key, Digital Signature.

જવાબ

જવાબ:

કોષ્ટક 5. Cryptographic ઘટકો

ઘટક	વ્યાખ્યા	ઉપયોગ
Public Key	ખુલ્લેઆમ શેર થતી encryption key	ડેટા એન્ક્રિપ્ટ, સહી ચકાસણી
Private Key	માલિક દ્વારા ગુપ્ત રખાતી key	ડેટા ડિક્રિપ્ટ, સહી કરવી
Digital Signature	સંદેશનો એન્ક્રિપ્ટેડ હેશ	અધિકૃતતા અને અખંડિતતા સાબિત કરવી

મેમરી ટ્રીક

જાહેર રક્ષણ કરે, ખાનગી સાબિત કરે (PPPP)

પ્રશ્ન 2(b) [4 ગુણ]

Explain Public blockchain with its advantage and disadvantage.

જવાબ

જવાબ:

કોષ્ટક 6. Public Blockchain વિશ્લેષણ

પાસું	વિગતો
વ્યાખ્યા	દરેક માટે ખુલ્લું નેટવર્ક
ઉદાહરણો	Bitcoin, Ethereum

ફાયદા:
- **પારદર્શિતા**: બધા વ્યવહારો જોઈ શકાય છે
- **વિકેન્દ્રીકરણ**: કોઈ એકનું નિયંત્રણ નથી
- **સુરક્ષા**: ઘણા નોડ્સ માન્ય કરે છે

ગેરફાયદા:
- **ઝડપ**: ધીમી પ્રક્રિયા
- **ઊર્જા**: ઉચ્ચ વીજળી વપરાશ
- **સ્કેલેબિલિટી**: પ્રતિ સેકન્ડ મર્યાદિત વ્યવહારો

મેમરી ટ્રીક

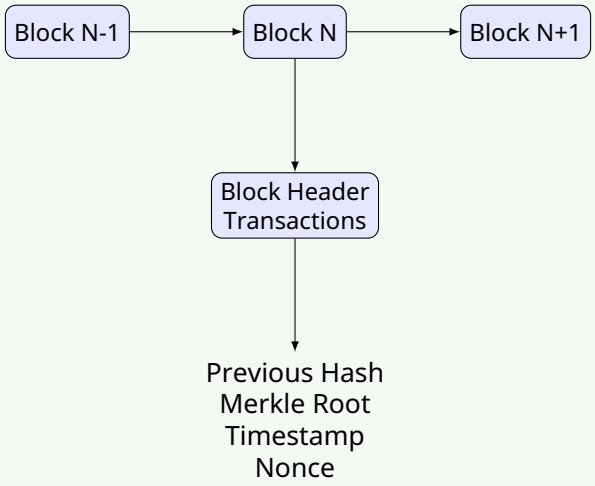
પારદર્શક પણ ધીમું (TBS)

પ્રશ્ન 2(c) [7 ગુણ]

Describe Core components of Blockchain.

જવાબ

જવાબ:
Blockchain માળખું



આકૃતિ 3. Core Blockchain ઘટકો

કોષ્ટક 7. Core ઘટકો

ઘટક	કાર્ય	મહત્વ
Block	વ્યવહારો માટે કન્ટેનર	ડેટા સંગ્રહ
Hash	અનન્ય ઓળખકર્તા	સુરક્ષા
Merkle Tree	વ્યવહાર સારાંશ	ચકાસણી
Nonce	માઇનિંગ નંબર	Proof of work
Timestamp	સમય રેકોર્ડ	કાલક્રમિક ક્રમ
Previous Hash	પાછલા બ્લોક સાથે લિંક	સાંકળ અખંડિતતા

- **અફરતા:** ભૂતકાળના રેકોર્ડ્સ બદલી શકાતા નથી
- **પારદર્શિતા:** બધો ડેટા દૃશ્યમાન
- **સહમતિ (Consensus):** નેટવર્ક માન્યતા પર સંમત થાય છે

મેમરી ટ્રીક

બ્લોક્સ હેશ મર્કલી નોન્સ સમય પાછલો (BHMNTP)

OR

પ્રશ્ન 2(a) [3 ગુણ]

Short Note on: SideChain

જવાબ

જવાબ:

કોષ્ટક 8. SideChain લક્ષણો

લક્ષણ	વર્ણન
વ્યાખ્યા	મુખ્ય બ્લોકચેન સાથે જોડાયેલ અલગ બ્લોકચેન
હેતુ	મુખ્ય બ્લોકચેન કાર્યક્ષમતા વધારવી
જોડાણ	Two-way peg મિકેનિઝમ

- **સ્કેલેબિલિટી**: મુખ્ય ચેઇનનો ભાર ઘટાડે છે
- **લવચીકતા**: કસ્ટમ ફીચર્સ શક્ય છે
- **સુરક્ષા**: મુખ્ય ચેઇન સુરક્ષા વારસામાં મેળવે છે

મેમરી ટ્રીક

અલગ સાઈડ સ્કેલ (SSS)

OR

પ્રશ્ન 2(b) [4 ગુણ]

Explain Private blockchain with its advantage and disadvantage.

જવાબ

જવાબ:

કોષ્ટક 9. Private Blockchain વિશ્લેષણ

પાસું	વિગતો
વ્યાખ્યા	નિયંત્રિત એક્સેસ સાથે પ્રતિબંધિત નેટવર્ક
નિયંત્રણ	એક જ સંસ્થા સંચાલન કરે છે

ફાયદા:
- **ઝડપ**: ઝડપી વ્યવહારો
- **ગોપનીયતા**: નિયંત્રિત ડેટા એક્સેસ
- **કાર્યક્ષમતા**: ઓછો ઊર્જા વપરાશ
- **Compliance**: નિયામક આવશ્યકતાઓ પૂરી કરે છે

ગેરફાયદા:
- **કેન્દ્રીકરણ**: નિયંત્રણનું એક બિંદુ
- **વિશ્વાસ**: નિયંત્રિત સંસ્થા પર આધાર રાખે છે
- **મર્યાદિત**: ઓછા સહભાગીઓ

મેમરી ટ્રીક

ઝડપી ખાનગી નિયંત્રિત (FPC)

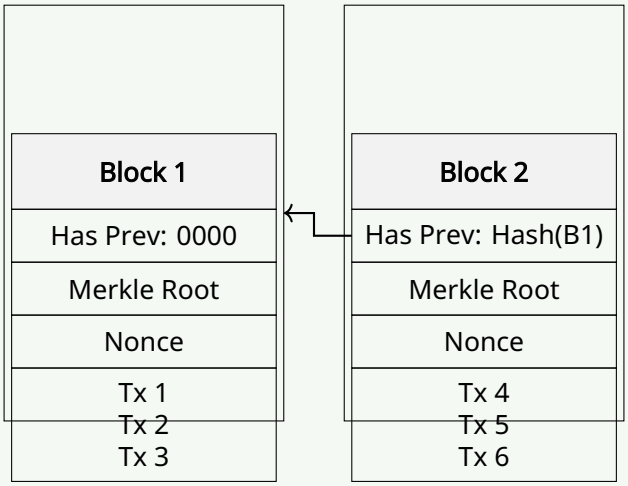
OR

પ્રશ્ન 2(c) [7 ગુણ]

Explain Data structure of Blockchain.

જવાબ

જવાબ:
Blockchain ડેટા સ્ટ્રક્ચર



આકૃતિ 4. Blockchain Linked List માળખું

કોષ્ટક 10. Data Structure તત્વો

તત્વ	હેતુ	સાઈઝ
Block Header	મેટાડેટા ધરાવે છે	Fixed size
Transaction List	વાસ્તવિક ડેટા	Variable size
Hash Pointer	બ્લોક્સ લિંક કરે છે	256 bits
Merkle Tree	વ્યવહાર સારાંશ	Logarithmic

મુખ્ય લક્ષણો:
- **રૈખિક માળખું**: બ્લોક્સ ક્રમમાં જોડાયેલા
- **Hash Linking**: દરેક બ્લોક પાછલા નો સંદર્ભ આપે છે
- **Merkle Trees**: કાર્યક્ષમ વ્યવહાર ચકાસણી
- **અફર**: શોધાયા વગર બદલી શકાતું નથી

મેમરી ટ્રીક

રૈખિક હેશ મર્કલી અફર (LHMI)

પ્રશ્ન 3(a) [3 ગુણ]

Short Note on: Consensus Mechanism in Blockchain.

જવાબ

જવાબ:

કોષ્ટક 11. Consensus Mechanism

પાસું	વર્ણન
હેતુ	નેટવર્ક સ્થિતિ પર સંમત થવું
જરૂરિયાત	Double spending અટકાવવું
પ્રકારો	PoW, PoS, DPoS

- **સંમતિ**: બધા નોડ્સ સંમત થવા જોઈએ
- **વિકેન્દ્રીકરણ**: કોઈ કેન્દ્રીય સત્તા નથી

- **સુરક્ષા**: દૂષિત પ્રવૃત્તિઓ અટકાવે છે

મેમરી ટ્રીક

સંમતિ સુરક્ષા અટકાવે (APS)

પ્રશ્ન 3(b) [4 ગુણ]

Compare Hard Fork and Soft Fork in Blockchain.

જવાબ

જવાબ:

કોષ્ટક 12. Fork તફાવત

લક્ષણ	Hard Fork	Soft Fork
સુસંગતતા	પછાત સુસંગત નથી (Not backward compatible)	પછાત સુસંગત (Backward compatible)
નિયમો	નવા નિયમો બનાવે છે	હાલના નિયમો કડક બનાવે છે
અપગ્રેડ	બધા નોડ્સ અપગ્રેડ કરવા પડે	વૈકલ્પિક અપગ્રેડ
પરિણામ	બે અલગ ચેઇન	એક ચેઇન ચાલુ રહે
ઉદાહરણ	Ethereum થી Ethereum Classic	Bitcoin SegWit

મુખ્ય તફાવતો:
- **Hard Fork**: બ્લોકચેનમાં કાયમી વિભાજન
- **Soft Fork**: કામચલાઉ પ્રતિબંધ જે કાયમી બને છે

મેમરી ટ્રીક

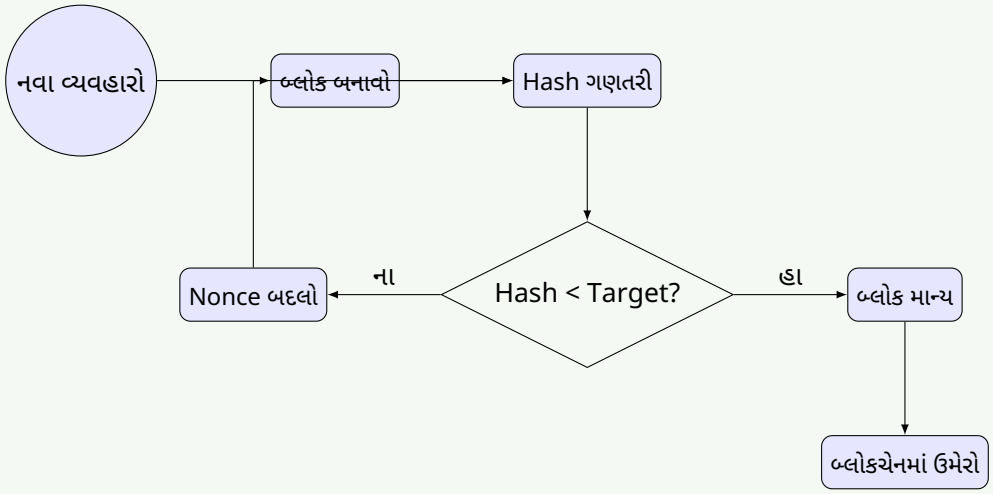
હાર્ડ સ્પ્લિટ, સોફ્ટ પ્રતિબંધ (HSSR)

પ્રશ્ન 3(c) [7 ગુણ]

What is Proof of Work? How does it work? Explain with example.

જવાબ

જવાબ:
Proof of Work પ્રક્રિયા



આકૃતિ 5. Mining અને PoW વર્કફ્લો

કોષ્ટક 13. PoW ઘટકો

ઘટક	કાર્ય	ઉદાહરણ
Hash Function	અનન્ય ફિંગરપ્રિન્ટ બનાવે છે	SHA-256
Nonce	Hash બદલવા માટે રેન્ડમ નંબર	12345
Difficulty	જરૂરી અગ્રણી શૂન્ય (zeros)	4 શૂન્ય
Mining	કમ્પ્યુટિંગ પ્રક્રિયા	Bitcoin mining

કાર્ય પ્રક્રિયા:
1. પેન્ડિંગ વ્યવહારો એકત્રિત કરો
2. વ્યવહારો સાથે બ્લોક બનાવો
3. વિવિધ nonce મૂલ્યો અજમાવો
4. વારંવાર hash ગણતરી કરો
5. જરૂરી શૂન્ય સાથે hash શોધો
6. નેટવર્ક પર માન્ય બ્લોક પ્રસારિત કરો

Bitcoin ઉદાહરણ:
- **Target**: Hash ચોક્કસ શૂન્યથી શરૂ થવું જોઈએ
- **Time**: 10 મિનિટ પ્રતિ બ્લોક
- **Reward**: 6.25 BTC (2024 મુજબ)

મેમરી ટ્રીક

અજમાવો ગણતરી કરો શૂન્ય સુધી (TCUZ)

OR

પ્રશ્ન 3(a) [3 ગુણ]

Short Note on: Block Rewards in Blockchain.

જવાબ

જવાબ:

કોષ્ટક 14. Block Rewards વિશ્લેષણ

લક્ષણ	વર્ણન
હેતુ	Miners ને પ્રોત્સાહન આપવા
ઘટકો	Block reward + transaction fees
Bitcoin	50 BTC થી શરૂ, દર 4 વર્ષે અડધું

- **પ્રેરણા**: નેટવર્ક સહભાગિતાને પ્રોત્સાહન આપે છે
- **અડધું કરવું**: સમય સાથે ફુગાવો ઘટાડે છે
- **ફી**: Miners માટે વધારાની આવક

મેમરી ટ્રીક

Miners પ્રેરિત પૈસા (MPP)

OR

પ્રશ્ન 3(b) [4 ગુણ]

What is 51% attack and how does it work?

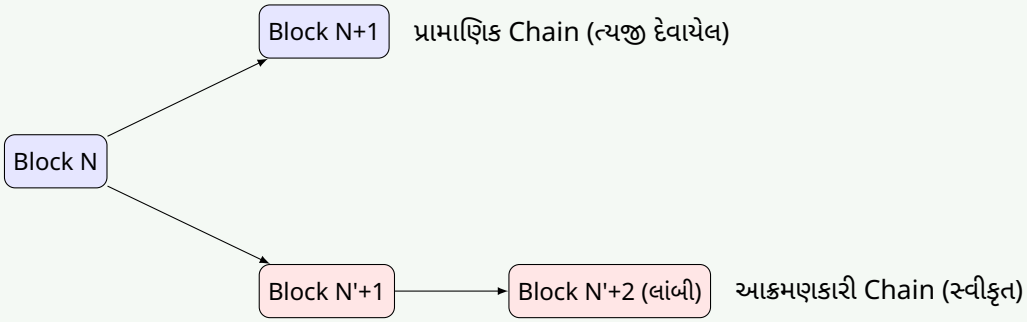
જવાબ

જવાબ:

કોષ્ટક 15. 51% Attack વિશ્લેષણ

પાસું	વિગતો
વ્યાખ્યા	બહુમતી mining power નિયંત્રિત કરવું
મર્યાદા	50% થી વધુ નેટવર્ક hash rate
ક્ષમતા	Transactions ઉલટાવી શકે છે
મર્યાદા	બીજાના coins ચોરી શકતો નથી

તે કેવી રીતે કામ કરે છે:
1. આક્રમણકારી બહુમતી mining power મેળવે છે
2. ખાનગી blockchain fork બનાવે છે
3. પ્રામાણિક નેટવર્ક કરતાં ઝડપથી mine કરે છે
4. નેટવર્ક પર લાંબી chain છોડે છે
5. નેટવર્ક લાંબી chain ને માન્ય તરીકે સ્વીકારે છે



આકૃતિ 6. 51% Attack મિકેનિઝમ

- **ડબલ ખર્ચ**: સમાન coins બે વાર ખર્ચ કરવા
- **Transaction ઉલટાવવા**: પુષ્ટિ થયેલા transactions રદ કરવા

મેમરી ટ્રીક

બહુમતી નિયંત્રણ Chain (BNC)

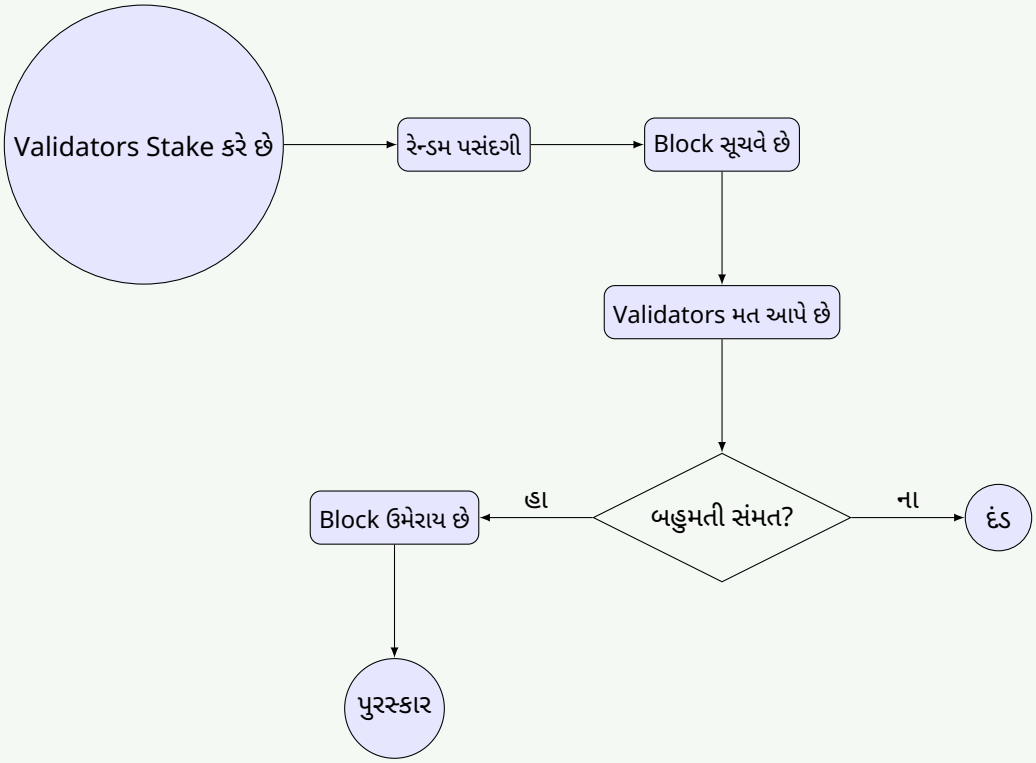
OR

પ્રશ્ન 3(c) [7 ગુણ]

What is Proof of Stake? How does it work? Explain with example.

જવાબ

જવાબ:
Proof of Stake પ્રક્રિયા



આકૃતિ 7. Proof of Stake વર્કફ્લો

કોષ્ટક 16. PoS vs PoW

લક્ષણ	Proof of Stake	Proof of Work
ઊર્જા	ઓછો વપરાશ	વધુ વપરાશ
પસંદગી	Stake આધારિત	Computing power
હાર્ડવેર	સામાન્ય કમ્પ્યુટર	વિશેષ miners
ઝડપ	ઝડપી	ધીમી

Ethereum ઉદાહરણ:
- **લઘુત્તમ Stake**: 32 ETH જરૂરી
- **દંડ**: દુષ્ટ વર્તન માટે slashing
- **ફાયદા**: ઊર્જા કાર્યક્ષમ અને સ્કેલેબલ

મેમરી ટ્રીક

Stake પસંદ Validate પુરસ્કાર (SPVP)

પ્રશ્ન 4(a) [3 ગુણ]

Describe Byzantine Fault Tolerance.

જવાબ

જવાબ:

કોષ્ટક 17. Byzantine Fault Tolerance

પાસું	વર્ણન
સમસ્યા	કેટલાક nodes દુષ્ટ રીતે વર્તે છે
સહનશીલતા	ખામીયુક્ત nodes છતાં સિસ્ટમ કામ કરે છે
આવશ્યકતા	1/3 થી ઓછા nodes ખામીયુક્ત હોઈ શકે છે

- **સર્વસંમતિ**: પ્રામાણિક nodes સંમત થવા જોઈએ
- **પ્રતિકાર**: નેટવર્ક હુમલાઓમાં ટકી રહે છે

મેમરી ટ્રીક

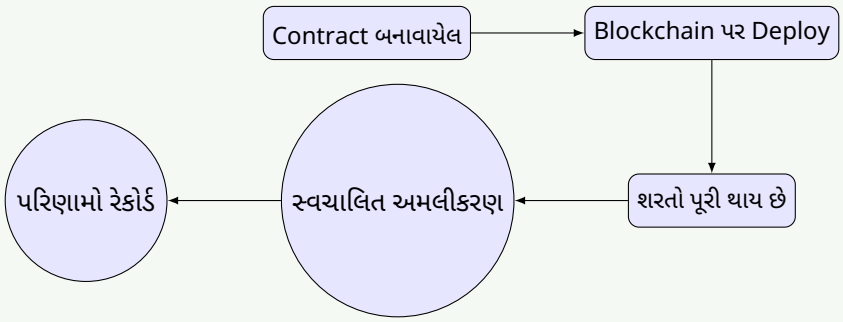
ખામીયુક્ત Nodes સહન (KNS)

પ્રશ્ન 4(b) [4 ગુણ]

How smart contract works in blockchain?

જવાબ

જવાબ:
Smart Contract અમલીકરણ



આકૃતિ 8. Smart Contract જીવનચક્ર

કાર્ય પ્રક્રિયા:
1. **નિર્માણ**: Developer contract code લખે છે
2. **Deployment**: Contract બ્લોકચેન પર સંગ્રહિત થાય છે
3. **Trigger**: બાહ્ય ઘટના contract સક્રિય કરે છે
4. **અમલીકરણ**: Code સ્વચાલિત રીતે ચાલે છે

મેમરી ટ્રીક

Code સ્વચાલિત અમલ (CSA)

પ્રશ્ન 4(c) [7 ગુણ]

What is SHA-256 and what is the use of SHA-256 in Blockchain.

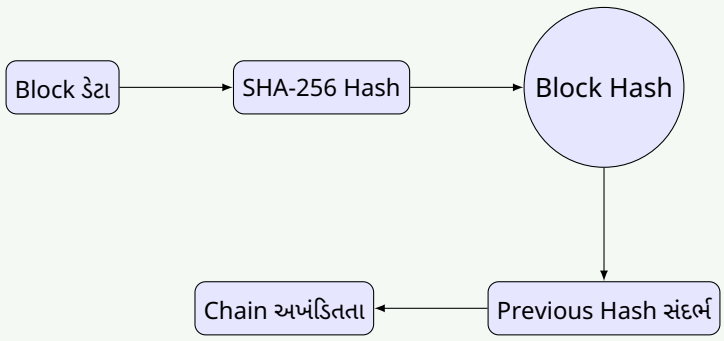
જવાબ

જવાબ:

કોષ્ટક 18. SHA-256 ગુણધર્મો

ગુણધર્મ	વર્ણન
પૂરું નામ	Secure Hash Algorithm 256-bit
આઉટપુટ	હંમેશા 256 bits (64 hex characters)
ઇનપુટ	કોઈ પણ કદનો ડેટા
પ્રકૃતિ	એક-માર્ગીય function

બ્લોકચેનમાં SHA-256



આકૃતિ 9. બ્લોકચેનમાં Hashing

બ્લોકચેનમાં ઉપયોગ:

- **Block Hashing**: ઉનિક block ઓળખકર્તા બનાવવા
- **Merkle Trees**: બધા transactions નો સારાંશ આપવા
- **Proof of Work**: Mining કઠિનતા લક્ષ્ય
- **Digital Signatures**: સુરક્ષિત transaction હસ્તાક્ષર

મેમરી ટ્રીક

Hash ઓળખે સુરક્ષિત કરે સાબિત કરે (HOSK)

OR

પ્રશ્ન 4(a) [3 ગુણ]

Explain Bitcoin and eventual consistency.

જવાબ

જવાબ:

કોષ્ટક 19. Bitcoin Consistency

ખ્યાલ	વર્ણન
Eventual Consistency	બધા nodes આખરે સંમત થાય છે
અસ્થાયી Forks	અનેક માન્ય chains અસ્તિત્વ ધરાવે છે
ઉકેલ	સૌથી લાંબી chain જીતે છે

- **સમય વિલંબ**: નેટવર્ક પ્રસારણમાં સમય લાગે છે
- **પુષ્ટિ**: વધુ blocks = વધુ નિશ્ચિતતા
- **અંતિમતા**: વ્યવહારિક રીતે અનુલટાવી શકાય તેવું બને છે

મેમરી ટ્રીક

આખરે દરેક સંમત (ADS)

OR

પ્રશ્ન 4(b) [4 ગુણ]

Discuss types of smart contract in blockchain.

જવાબ

જવાબ:

કોષ્ટક 20. Smart Contract પ્રકારો

પ્રકાર	કાર્ય	ઉદાહરણ
કાનૂની Contract	કાનૂની રીતે બંધનકર્તા કરાર	Real estate ટ્રાન્સફર
Application Logic	Decentralized app functions	Token એક્સચેન્જ
Decentralized Autonomous	સ્વ-શાસિત સંસ્થાઓ	DAO મતદાન
Multi-signature	અનેક મંજૂરીઓ જરૂરી	Escrow સેવાઓ

મેમરી ટ્રીક

કાનૂની Logic સ્વાયત્ત બહુ (KLSB)

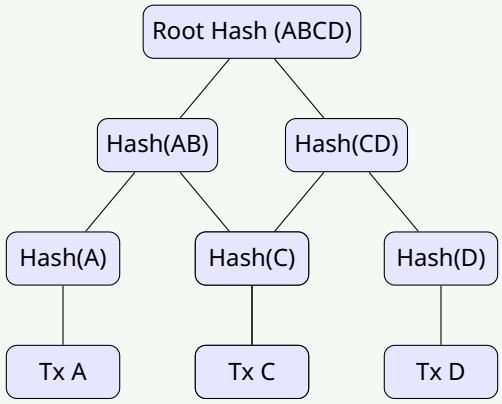
OR

પ્રશ્ન 4(c) [7 ગુણ]

Define Merkle Tree and explain how it works in blockchain.

જવાબ

જવાબ:
Merkle Tree રચના



આકૃતિ 10. Merkle Binary Tree

કોષ્ટક 21. Merkle Tree ફાયદા

ફાયદો	વર્ણન
કાર્યક્ષમતા	બધો ડેટા ડાઉનલોડ કર્યા વિના transactions ચકાસો
સુરક્ષા	કોઈ પણ ફેરફાર તરત શોધાય જાય છે
સ્કેલેબિલિટી	Logarithmic ચકાસણી સમય
સંગ્રહ	કોમ્પેક્ટ પ્રતિનિધિત્વ

કાર્ય પ્રક્રિયા:
1. **Hash Transactions**: દરેક transaction નો hash મેળવો
2. **જોડી Hashing**: નજીકના hashes ને મિલાવો
3. **પ્રક્રિયા પુનરાવર્તન**: એક root hash સુધી ચાલુ રાખો
4. **Root સંગ્રહ**: ફક્ત root block header માં સંગ્રહિત કરો

મેમરી ટ્રીક

Tree ગોઠવે ચકાસે કાર્યક્ષમ રીતે (TGCK)

પ્રશ્ન 5(a) [3 ગુણ]

Short Note on: Bitcoin Scripting

જવાબ

જવાબ:

કોષ્ટક 22. Bitcoin Scripting

લક્ષણ	વર્ણન
ભાષા	Stack-based programming ભાષા
હેતુ	ખર્ચની શરતો વ્યાખ્યાયિત કરવી
અમલીકરણ	Coins ખર્ચ કરવામાં આવે ત્યારે ચાલે છે

- **સરળ**: ફક્ત મૂળભૂત operations
- **સુરક્ષિત**: મર્યાદિત કાર્યક્ષમતા દુરુપયોગ અટકાવે છે
- **લવચીક**: વિવિધ transaction પ્રકારો શક્ય છે

મેમરી ટ્રીક

Stack વ્યાખ્યા ખર્ચ (SVK)

પ્રશ્ન 5(b) [4 ગુણ]

Explain Decentralized Applications (dApps) in Blockchain and how does it work?

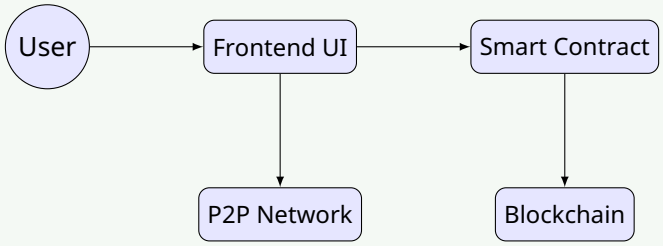
જવાબ

જવાબ:

કોષ્ટક 23. dApp ઘટકો

ઘટક	કાર્ય
Frontend	User interface
Backend	Blockchain પર smart contracts
Storage	Decentralized storage systems
Network	Peer-to-peer communication

dApp Architecture



આકૃતિ 11. dApp વર્કિંગ મોડેલ

મુખ્ય લક્ષણો:
- **કોઈ કેન્દ્રીય સર્વર નથી**: વિતરિત નેટવર્ક પર ચાલે છે
- **Open Source**: Code જાહેરમાં ઉપલબ્ધ છે
- **સ્વાયત્ત**: કંપની નિયંત્રણ વિના કામ કરે છે

મેમરી ટ્રીક

વિકેન્દ્રીત Apps દરેક જગ્યાએ ચાલે (VADJ)

પ્રશ્ન 5(c) [7 ગુણ]

Explain Hyperledger with its advantages and disadvantages.

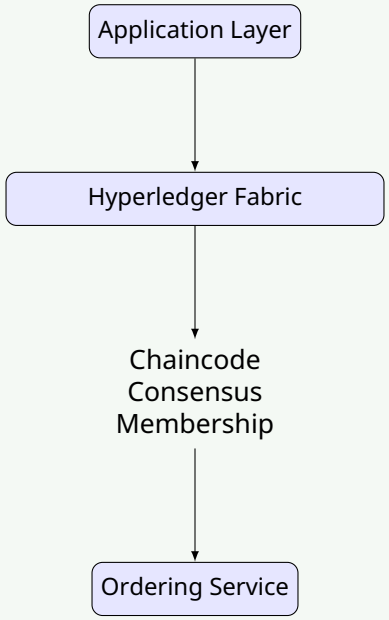
જવાબ

જવાબ:

કોષ્ટક 24. Hyperledger ઝાંખી

પાસું	વર્ણન
પ્રકાર	Private/Consortium blockchain platform
વિકાસકર્તા	Linux Foundation
લક્ષ્ય	Enterprise applications
Consensus	Pluggable consensus mechanism

Hyperledger આર્કિટેક્ચર



આકૃતિ 12. Hyperledger Layered આર્કિટેક્ચર

ફાયદા:
- **પ્રદર્શન**: ઉચ્ચ transaction throughput
- **ગોપનીયતા**: ગુપ્ત transactions
- **મોડ્યુલર**: Pluggable components

ગેરફાયદા:
- **કેન્દ્રીકરણ**: સંપૂર્ણ વિકેન્દ્રીકૃત નથી
- **જટિલતા**: સેટ કરવું મુશ્કેલ છે
- **ખર્ચ**: મોંઘું infrastructure

મેમરી ટ્રીક

ખાનગી પ્રદર્શન Enterprise (KPE)

OR

પ્રશ્ન 5(a) [3 ગુણ]

Short Note on: Bitcoin Mining

જવાબ

જવાબ:

કોષ્ટક 25. Bitcoin Mining વિશ્લેષણ

પાસું	વર્ણન
હેતુ	Transactions ચકાસણી અને blocks બનાવવા
પ્રક્રિયા	Cryptographic પઝલ હલ કરવા
પુરસ્કાર	BTC + transaction fees

- **હાર્ડવેર**: વિશિષ્ટ ASIC miners
- **ઊર્જા** : ઉચ્ચ વીજળી વપરાશ
- **સ્પર્ધા**: વૈશ્વિક mining pools સ્પર્ધા કરે છે

મેમરી ટ્રીક

ચકાસણી હલ પુરસ્કાર (CHP)

OR

પ્રશ્ન 5(b) [4 ગુણ]

Short Note on: Decentralized Autonomous Organization (DAO)

જવાબ

જવાબ:

કોષ્ટક 26. DAO લક્ષણો

લક્ષણ	વર્ણન
ગવર્નન્સ	સમુદાય-સંચાલિત નિર્ણયો
મતદાન	Token-આધારિત મતદાન અધિકારો
સ્વચાલન	Smart contracts નિર્ણયો અમલ કરે છે
પારદર્શિતા	બધી પ્રવૃત્તિઓ બ્લોકચેન પર

મુખ્ય લાક્ષણિકતાઓ:
- **કોઈ કેન્દ્રીય સત્તા નથી**: સમુદાય નિયંત્રિત
- **Token માલિકી**: Tokens આધારે મતદાન શક્તિ
- **સ્વચાલિત અમલીકરણ**: મંજૂર પ્રસ્તાવો સ્વચાલિત અમલ થાય છે

મેમરી ટ્રીક

સમુદાય મત આપે સ્વચાલિત (SMS)

OR

પ્રશ્ન 5(c) [7 ગુણ]

Explain ERC-20 with its advantages and disadvantages

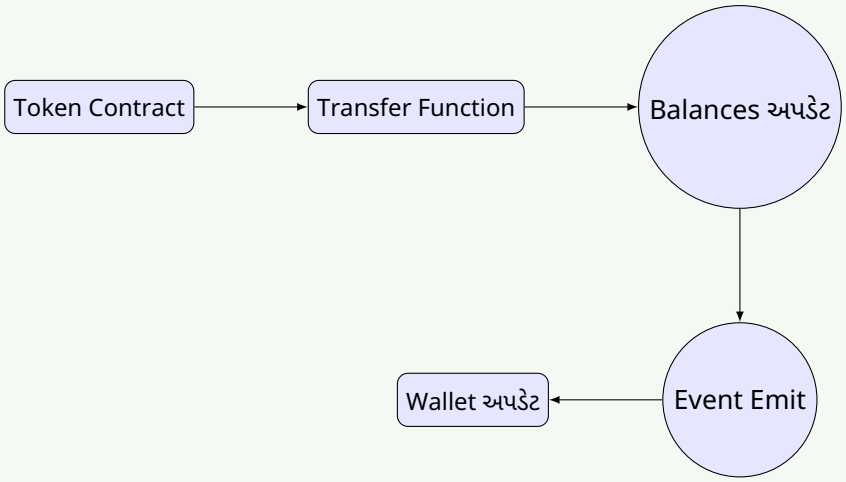
જવાબ

જવાબ:

કોષ્ટક 27. ERC-20 Standard ઝાંખી

પાસું	વર્ણન
પૂરું નામ	Ethereum Request for Comments 20
પ્રકાર	Ethereum પર token standard
Functions	માનકીકૃત token operations
સુસંગતતા	બધા Ethereum wallets સાથે કામ કરે છે

ERC-20 Token Flow



આકૃતિ 13. ERC-20 Execution Flow

જરૂરી Functions:

કોષ્ટક 28. જરૂરી Functions

Function	હેતુ
totalSupply()	કુલ token supply પરત કરે
balanceOf()	Account balance ચકાસે
transfer()	Address પર tokens મોકલે
approve()	વતી ખર્ચની મંજૂરી આપે

ફાયદા:
- **માનકીકરણ**: બધા tokens માટે એકસમાન interface
- **Interoperability**: કોઈ પણ Ethereum wallet/exchange સાથે કામ કરે છે
- **Liquidity**: Decentralized exchanges પર ટ્રેડ કરી શકાય છે

ગેરફાયદા:
- **Gas Fees**: Ethereum transaction ખર્ચ
- **સ્કેલેબિલિટી**: નેટવર્ક congestion સમસ્યાઓ
- **સુરક્ષા**: Smart contract vulnerabilities

મેમરી ટ્રીક

Standard Tokens Trade Everywhere (STTE)