Test Exam

What is the genesis block ?
- Any block created by the founder
- The last block created in the Blockchain
- The first block of a Blockchain
- The first transaction in each block

In Bitcoin a block is produced every :
- 2 weeks
- 20 minutes
- 2016 minutes
- 10 minutes

The transaction Merkle Tree root value in a Bitcoin block is calculated using,
- Hash of transactions
- Previous block's hash
- Number of transactions
- None of the above

Where is a Blockchain's central server?
- Where the blockchain is created
- Located with the owner of the server
- There is no central server, it is distributed
- Ordered Node

The main properties of blockchain are ?
- Decentralization
- Immutability
- Transparency
- All of the above

The generation of multiple branchs in blockchain is called,
- Division
- Merge
- Fork
- None of the above

Given a message M and a hash function H
- Knowing H(M), one can compute M
- Knowing M, one can compute H(M)
- H(M) and M always have the same size
- It is guaranteed that H(H(M)) = M

What key must be used by Bob to be certain that only Alice can read the message that Bob wants to send her?
- Bob public key
- Alice private key
- Alice public key
- Bob private key

What is the hashing algorithm used in bitcoin?
- MD5
- Keccak-256
- SHA-256
- RIPEMD-160

In Ethereum the EOA is,
- controlled by a contract code
- controlled by a private key
- 160-bits length
- 256-bits length

Full node does not,
- Maintains a complete copy of the blockchain
- Mines block
- Verify all transactions
- adds it to the blockchain

The mining in bitcoin consists to find a nounce value that will make the first k bits of its n hash bits to zero, i.e., finding hash values that are smaller than or equal to a certain target value. Suppose that n=8 and k=3, so the target value is,
- 29 - 30 - 31 - 32

In elliptic curve, we assume that after several iterations we obtain 17P+P = Ø, we say that,
- 17P is the opposite of P
- 17P is the inverse of P
- P is the inverse of 17P
- 17P is the primitive of P

In the smart contract program we must explicitly specify the constructor
- True
- False

In digital signature, a valid signature must verify,
- Verify(pk,message,sign(sk,message))==true
- Verify(pk,message,sig)==true
- Verify(pk,message,sk,message)==true
- Verify(pk,message,sk)==true

The earliest deployed consensus algorithms are :
- Bitcoin-NG, PoW, PBFT
- PoS, Algorand, PoW
- DAG-based, PoW, PoS
- PoW, PoS, PBFT

The smart contract deployment process consists of :
- Generating the ABI
- Generating the Byte code
- Compiling the smart contract
- None of the above

web3.js allow the frontend to communicate with an ethereum node via,
- servlet
- JSON-RPC
- Websocket
- HTTP

const web3 = new Web3('http://127.0.0.1:7545'); indicate that we will use the blockchain :
- Remix
- Web3.js
- Ganache
- HTTP

The function *web3.eth.sendTransaction* is used to :
- Transfert ether between account
- Send transaction
- Get the list of transactions
- Get the arguments of the transactions