

CBDE.VCEplus.premium.exam.102q

Number: CBDE  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1.0



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

CBDE

BTA Certified Blockchain Developer - Ethereum



## Exam A

### QUESTION 1

Consensus is reached:

- A. by the miner nodes which make sure that a transaction is valid.
- B. by every single node in the blockchain network executing the same transaction.
- C. by a cryptographic secure signature algorithm called ECDSA which makes sure that cheating is impossible.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 2 Smart Contracts

can be written in:

- A. Java, C++, Solidity and JavaScript, because the Ethereum Blockchain is completely language agnostic and cross compilers exist for every major language.
- B. Solidity, Viper, LLL and Serpent, because those are high level languages that are compiled down to bytecode.
- C. Solidity and JavaScript, because those are the official first implementations for Distributed applications and the Blockchain supports those languages fully.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 3 Solidity

gets compiled:

- A. to bytecode that can't be understood by humans.
- B. to bytecodes which are essentially opcodes running instruction by instruction.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 4 Having a bug-bounty

program early on:

- A. can help to engage the community in testing your smart contracts and therefore help to find bugs early.
- B. might be a burden as it is an administrative overhead mainly.
- C. is completely useless. Who wants to test beta-ware software? It's better to start with the bug-bounty program after the contract is released on the main-net.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 5

Which is the right order for Denominations?

- A. Wei, Finney, Szabo, Ether, Tether.
- B. Finney, Szabo, Mether, Gwei.
- C. Gwei, Szabo, Finney, Ether.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 6** The nonce-field in a transaction is used:

- A. to protect against replay attacks.
- B. to have an additional checksum for transactions.
- C. to sum up all ethers sent from that address.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 7** Which statement is true about the EVM?

- A. While the EVM is Sandboxed, it isn't as powerful as the Bitcoin Network, because it's not Turing Complete.
- B. The EVM can't access hardware layers or anything outside a blockchain node because it's sandboxed.
- C. The EVM is extremely powerful, turing complete and perfect for doing computational intensive things, because of the direct access to the graphics card.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

DApps are:

- A. great, because they cut the middle man, run on a trusted platform, apply logic to the blockchain where already economic assets are running and thus allow peer to peer trade.
- B. an amazing way to create new applications. Those applications run entirely separated from other applications on the platform and allow for logical interactions. They can't access any funds to add an additional layer of trust.
- C. a new way of applying logical operations for banks and big financial institutions. This way they can reduce the staff while operating at increased security.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 9** To get most out of the blockchain, it is best:

- A. to use it for the whole business logic. It's always best to have everything in once place.
- B. to use it only for things which need the benefits of the blockchain.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 10** A Hashing Algorithm is deterministic. What does it mean?

- A. it always produces the same output given the same input.
- B. it uses equally distributed data to produce the output given a long input.
- C. it shouldn't be possible to re-generate the input given the output.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11** What's the correct scientific notation?

- A. 1 Ether =  $10^{18}$  wei,  $10^9$  Gwei,  $10^3$  Finney
- B. 1 Ether =  $10^{19}$  wei,  $10^{13}$  Gwei,  $10^3$  Finney
- C. 1 Ether =  $10^{16}$  wei,  $10^{13}$  Gwei,  $10^3$  Finney
- D. 1 Ether =  $10^{18}$  wei,  $10^6$  Gwei,  $10^6$  Finney



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 12** What are Private Keys used for?

- A. To Protect the Public Keys by being cryptographically significant.
- B. To Sign Transactions And To Derive an Address From.
- C. To Generate An Address which can sign transactions.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 13** Public Keys vs. Private Keys. Which statement is true?

- A. The Public Key is for Signing Transactions, the Private Key must be given out to verify the signature.

- B. The Private Key signs transactions, the Public Key can verify the signature.
- C. The Private Key is to generate a Public Key. The Public Key can sign transactions, the address is here to verify the transactions.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14** Proof of Work (PoW) vs.  
Proof of Stake.

- A. PoW is computationally intensive which requires lots of energy. On the other hand, miners earn straightforward a reward for mining a block and incorporating transactions.
- B. PoW is better than PoS, because with PoS we increase the amount of energy spent on the network.
- C. PoS is mining with specialized new hardware that has to be purchased with a stack of Ether in the network. Hence the Name: Proof of Stake, which derives from Stack.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 15** Externally  
Owned Accounts:

- A. can be destroyed using the selfdestruct keyword. This way all remaining ether will be sent to the receiver address, regardless if they have a fallback function or not.
- B. are bound to a private key which is necessary to sign transactions outgoing from that account.
- C. are logical opcodes running on the ethereum blockchain very similar to smart contracts.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

Smart Contracts:

- A. are always living on the same address, because the blockchain is deterministic. So, one account can always have one smart contract.
- B. are having the same address as the EOA.
- C. are sitting on their own address. The Address is created from the nonce and the EOA address and could be known in advance before deploying the smart contract.
- D. the address of the smart contract is a random address which gets generated by the miner who mines the contract-creation transaction.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 17** Transactions containing the same data to create the same  
smart contract are:

- A. always having the same signature.
- B. having a different signature because of the nonce which changes upon every transaction.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 18** Sending one Ether is actually internally translated:

- A. to Wei, so it will send the equivalent of  $10^{18}$  Wei.
- B. to Finney, so it will send the equivalent of  $10^3$  Finney.
- C. to Szabo, so it will send the equivalent of  $10^6$  Szabo.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

Hashing Mining uses:

- A. Keccak256 while internally to hash values it's easy to use the Dagger-Hashimoto to create a meaningful hash.
- B. the Dagger-Hashimoto hashing while internally the EVM uses SHA256 which is an alias for Keccak256.
- C. the Dagger-Hashimoto hashing while internally the EVM uses Keccak256 which is almost similar to SHA256, but has a different padding so produces different hashes.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

PoS:

- A. would be better, because it can reduce the amount of energy needed for mining.
- B. would be worse, because it would increase the amount of energy needed for mining.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 21** Externally Owned

Accounts (EoA):

- A. are changing their address every time a Transaction is sent because of the nonce.
- B. are keeping their address, but on the blockchain a nonce is increased every time they send a transaction to avoid replay attacks.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 22**

What are Ethereum Nodes?

- A. Programs implementing the Ethereum Protocol to talk to each other and JSON-RPC interfaces to talk to the outside world.
- B. A Java-Script library to compile and run Solidity Code.
- C. A Framework for deploying and running smart contract in a decentralized way.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 23** To communicate with an Ethereum node via JavaScript:

- A. the library you use must make use of the JSON-RPC Interface of an Ethereum Node.
- B. must Implement the Ethereum Protocol to connect to other Ethereum Nodes.
- C. must use Web3.js, which is closed source to communicate to other Ethereum Nodes.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 24** It's possible to access the blockchain via an Ethereum Node:

- A. only via JavaScript because there is the proprietary Web3.js library.
- B. by any programming language, as long as it adheres to the JSON-RPC standard.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 25** A

Private Network is:

- A. a side Channel to the Ethereum Main Net which costs less gas to run smart contracts.
- B. an exact clone of the Rinkeby Test-Network which can be started as virtual machine in the Azure Cloud.
- C. a Network running only in a private area, where people cannot join freely and openly.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 26** For Rapid Development

Cycles it's good:

- A. to deploy to the main-network as quickly as possible.

- B. to use in-memory blockchain simulations, because mining works instantaneously.
- C. to use a private network at all times, because this is the closest you get to the real network.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 27

Go-Ethereum vs. Ganache:

- A. both are the same, just implemented in a different language.
- B. with Go-Ethereum you get a real blockchain node where you can create your own local private network, connect to Test-Networks or the Main-Net, while with Ganache you get an in-memory blockchain simulation.
- C. with Ganache you get a real blockchain node where you can connect to the Test-Networks Rinkeby and Ropsten.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 28

Block Timestamp:

- A. the timestamp is based on the time zone of the miner, that is why it changes the difficulty continuously to reflect network latency.
- B. the timestamp can't be influenced by a miner and is generally considered safe to be used for randomness on the blockchain.
- C. the timestamp can be influenced by a miner to a certain degree but it's always independent from the time-zone.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 29

Block Difficulty:

- A. is determined by the Ethereum Committee every fortnight to reflect the average amount of transaction and it cannot be influenced by the network itself.
- B. increases when the time between mined blocks is below 10 seconds, while it decreases when the time is above 20 seconds.
- C. increases when the time between mined blocks is below 20 seconds, while it decreases when the time is above 60 seconds.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 30

Ethereum Nodes:

- A. must implement the Ethereum protocol and external access can only be done via the proprietary Ethereum Libraries like Web3.js.
- B. must implement the Ethereum Protocol and a JSON-RPC to talk with clients.
- C. must implement Web3.js to interact with Websites.



**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 31** When a new block is mined:

- A. a list of transactions as well as uncles is incorporated in the block. All gas that is used during those transactions is added to the miners' balance. Also, the block reward is added to the miner. Then the same transactions are run again by every participating node in the network to achieve consensus.
- B. a list of transactions is incorporated in that block. Gas used during the execution is attached to the executing contracts while the block reward is automatically spread across the mining pool to ensure a fair spread. Consensus is reached by a special form of hash code.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 32** A Blockchain Node:

- A. can never become a mining node.
- B. can always become a mining node.
- C. can become a mining node, depending if the implementation has the functionality implemented.

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 33** On a consortium network:

- A. everybody can become a miner, everybody can send transactions and everything is public.
- B. usually only a few selected nodes can be miners. Transactions can be further limited.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 34** The JSON-RPC Protocol:

- A. is used to communicate between blockchain nodes.
- B. is used to ensure safe communication between miners.
- C. is a mean of dumping the blockchain data in a so-called consensus export.
- D. is used to communicate between the blockchain node and externally running applications.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

GETH:

- A. is the reference implementation of the Ethereum protocol and every other node implementation internally uses the closed-source from Geth.
- B. is the library that is used for the blockchain node Go-Ethereum. It is also used by Parity is parts, because it's closed source.
- C. is one of the many blockchain nodes that implement the Ethereum Protocol. It's open source and everyone can contribute.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 36** To store almost all data in the Ethereum Blockchain:

- A. a Linked List with pointers to previous blocks hashes is used.
- B. a Merkle Patricia Trie is used.
- C. a Radix Trie is used because the Merkle Patricia Trie is too inefficient.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 37** You interact with a smart contract and see a gas usage of 50,000 gas with a gas cost of 15Gwei.

How much Ether would you have to pay to the miner?

- A. 750,000,000,000,000 Wei
- B. 750,000,000,000 Wei
- C. 750,000,000 Wei
- D. A flat fee of 1 Ether

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 38** Checking the balance of an address inside a loop of a smart contract constantly:

- A. doesn't cost any gas.
- B. cost gas every time we check the balance.

**Correct Answer: B**

**Section: (none)**

**Explanation****Explanation/Reference:**

**QUESTION 39** Gas costs accrue on sending a transaction:

- A. no matter the content.
- B. only with a new smart contract deployment.
- C. only interacting with an already deployed smart contract.

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 40**

EVM assembly:

- A. is much better than Solidity and a viable alternative.
- B. can be split across multiple files, but every contract must be in a file with the same name as the contract itself.
- C. is another language similar to LLL, more secure than Solidity.

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 41**

Solidity files:

- A. can't be split across multiple files, everything should be in one single file.
- B. can be split across multiple files, but every contract must be in a file with the same name as the contract itself.
- C. can be spread across multiple files. To import all contract from a file you can use "import 'myfile.sol'. To import Contract MyContract from myfile.sol you use "import {MyContract as SomeContract} from 'myfile.sol';".

**Correct Answer:** C

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 42**

Files

can be imported:

- A. using relative and absolute paths, where the "." And the ".." depict that it's a relative path.
- B. only via GitHub using the Repository and Username.
- C. using the special requirefile(...) statement, which looks in a specific library path to import files.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

Importing from GitHub:

- A. works across all compilers and platforms the same way.
- B. is generally possible, but currently works only in Remix, but doesn't work in Truffle.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 44** Single line

comments in Solidity are:

- A. working with either // or ///
- B. working with /\* comment \*/ or /\*\* @.. natspec style \*/
- C. not possible, all comments must be multi-line.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 45** Multi-Line

Comments in Solidity are:

- A. working with either // or ///
- B. working with /\* comment \*/ or /\*\* @.. natspec style \*/
- C. not possible, all comments must be single-line.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 46** The following are value

types in Solidity.

- A. Integer, Boolean, Struct, Mapping and Enum.
- B. Integer, Boolean, Enum and Addresses.
- C. Integer, Boolean, Structs and Fixed Point Numbers.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 47**

To compare a String in Solidity you use:



- A. `string1 == string2`
- B. the internal function `"str_compare(str1,str2)"`
- C. you can't directly compare two strings, but one method would be to hash both strings and compare the hashes.
- D. `bytes32(string1) == bytes32(string2)`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 48** If we divide two integers:  
5/2, the result is:

- A. 2, because the decimal is truncated.
- B. 3, because it's always rounded.
- C. 2.5, because it's automatically converted into a float.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 49** A

Struct is a great way:

- A. to define a new datatype in Solidity, so you don't need to use objects of another contract.
- B. to hold instances of other contracts.
- C. to implement pointers to other contracts that can hold new datatypes.



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 50** A Mapping consists of  
keys and value.

- A. the Keys can be anything, but the value can't be another mapping or struct.
- B. the Value can be anything, but the key cannot be another mapping, struct, integer or Boolean.
- C. the value can be anything, but the key cannot be another mapping, struct, enum or dynamically sized array.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

To iterate through a mapping, you:

- A. can use the length parameter of the mapping.

- B. you need an external helper variable.
- C. you cannot iterate any mapping to make the overall language design more safe.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 52** Function and Variable Visibility:

- A. a function that is marked as internal cannot be called by other contracts, unless the function is used by a derived contract. Private Functions cannot be called by any other outside contract and public variables are generating automatically a getter function.
- B. a function that is marked as external can never be called internally. Private functions can also be called by derived contracts using inheritance. Private variables are accessible also in derived contracts.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 53** View and Pure Functions:

- A. a function marked as pure can change the state, while a view function can only return static calls.
- B. a function marked as view can never access state variables, while pure functions are here to return only one value.
- C. a view function can access state variables, but not write to them. A Pure function cannot modify or read from state.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 54** View and Pure Functions:

- A. can only be accessed during calls.
- B. can be accessed during transactions and calls.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 55** The Fallback function:

- A. cannot receive Ether, not even by adding the payable modifier.
- B. can contain as much logic as you want, but it's better to keep it short and not exceed the gas stipend of 2300 gas.
- C. can be used to avoid receiving ether.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 56** You need to use \_\_\_\_\_ to get the address that initiated the transaction.

- A. Tx.origin
- B. Msg.sender

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 57** If a User calls contract A and that calls Contract B, then msg.sender in Contract B will contain the address of:

- A. the User.
- B. contract A.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 58**

Loops in Solidity:

- A. are a great way to circumvent gas requirements, because a loop will only consume gas once.
- B. are dangerous when used with data structures that grow, such as arrays or mapping, because it is hard to estimate the gas requirements.
- C. should be avoided where possible, because of unknown side-effects on the gas requirements.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

Events:

- A. are stored on chain and are a great way to get a return value when a contract calls another contract.
- B. are stored in something like a side-chain and cannot be accessed by contracts.
- C. are used primarily for debugging exceptions in solidity.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 60** According to the official Style Guide:

- A. you should capitalize function names, events and contract names, to avoid confusion with JavaScript. You should use Tabs to indentation and a maximum of 80 characters per line.
- B. contract names should be capitalized, while functions should be mixedCase. You should use 4 spaces as indentation and a maximum of 79 (or 99) characters per line.
- C. contract should be mixedCase, as well as function names. Events should be capitalized. 2 spaces should be used as indentation and a maximum of 120 characters per line.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 61** A version pragma is a great way to make it clear:

- A. for which compiler version a smart contract was developed for. It helps to avoid breaking changes.
- B. for which blockchain a smart contract was developed for. It helps to avoid confusion with beta-customers.
- C. for which blockchain node a smart contract was developed for. It helps to avoid mixing up different versions of go-ethereum.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 62** Variables of the type address store:

- A. a 20 bytes value
- B. a 32 bytes value
- C. a string
- D. a 20 characters long hex number

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

Address.send():

- A. will cascade exceptions and address.transfer() will return a false on error.
- B. will return false on error while address.transfer() will cascade transactions.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

Address.call.value():



- A. sends the gas stipend of 2300 gas and returns a false on error.
- B. sends all the gas along and cascades exceptions.
- C. sends all the gas along and returns a false on error.
- D. sends the gas stipend of 2300 gas and cascades exceptions.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 65** Address.send() and address.transfer() are considered:

- A. safe against reentrancy because of the small gas stipend of 2300 gas.
- B. dangerous because they send all gas along, it's better to use address.call.value()).

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 66** When defining a new datatype:

- A. its best to use a contract with public storage variables, so it can be used like a class.
- B. it's best to use a struct, which is cheaper than deploying a new contract.
- C. it's not possible to generate new datatypes in Solidity.



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

What's the difference between Ethereum Request for Comments (ERC) and Ethereum Improvement Proposals (EIP)?

- A. ERC are here to define standards for the usage of Ethereum. EIP are here to improve the Ethereum Protocol itself.
- B. ERC are here to propose new distributed applications on top of the Ethereum layer, while EIP are here to improve existing mining software.
- C. ERC are an open platform to discuss continuous forking of the Ethereum platform. Successful forks are then incorporated in the EIP for further voting by the Ethereum Consortium.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 68** What is the difference between ERC20 and ERC721 Tokens in simple terms?

- A. The tokens of a certain ERC20 symbol are all the same, the tokens of an ERC721 symbol are all different. So, ERC20 tokens are fungible, while ERC721 tokens are non-fungible.

B. The tokens of a certain ERC20 symbol are all different, the tokens of an ERC721 symbol are all the same. So, ERC20 tokens are non-fungible while ERC721 tokens are fungible.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 69

In order to implement an ERC20 token contract, you'd need at least to implement the following functions and events in order to fulfill the interface requirements:

- A. totalSupply(), balanceOf(address), allowance(address,address), transfer(address,uint256), approve(address,uint256), transferFrom(address,address,uint256). Events: Transfer(address,address,uint256), Approval(address,address,uint256)
- B. name(), symbol(), totalSupply(), balanceOf(address), ownerOf(uint26),approve(address,uint256), takeOwnership(uint256),transfer(address,uint256),Events: Transfer(address,address,uint256), Approval(address,address,uint256)

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 70** Why is it important to follow the same Interfaces?

- A. Websites that try to interface with the Token would have to know the exact ABI. It is upfront clear how the interaction has to be with the standard Interfaces.
- B. The Ethereum Foundation can easily validate the Tokens and approve any audits by following the standard interface.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 71** If contract MyContractA is derived from Contract MyContractB, then this would be the right syntax:

- A. contract MyContractA is MyContractB { ... }
- B. contract MyContractA inherit (MyContractB) {...}
- C. contract MyContractA extends MyContractB {...}
- D. contract MyContractB derives MyContractA {...}

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 72** Inheritance is useful, because a contract that is derived from another contract can make use of:

- A. all public state variables and properties, public and internal functions and modifiers.
- B. all public and private state variables, public, internal and external functions, but not modifiers
- C. all public state variables and properties, public functions and modifiers, but not internal, external or private ones.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 73** Finish the sentence: The Library Web3.js is ....:

- A. useful when developing distributed applications with HTML and JavaScript, because it already implements the abstraction of the JSON-RPC interface of Ethereum Nodes.
- B. necessary when developing distributed applications with HTML and JavaScript, because the proprietary JSON-RPC interface of Ethereum Nodes is a closed source.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 74** When solidity is compiled then also Metadata is generated:

- A. the Metadata contains the ABI Array, which defines the Interface to interact with the Smart Contract. Metadata can also contain the address of the smart contract when it gets deployed.
- B. metadata contains the address, and the size of the smart contract. The ABI Array is generated externally upon deploying the smart contract.
- C. the ABI array and the Metadata are not generated when solidity is compiled to bytecode, its generated by a migration software which deploys the smart contract on the blockchain.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



**QUESTION 75** The difference between address.send() and address.transfer() is:

- A. .send returns a Boolean and .transfer throws an exception on error. Both just forward the gasstipend of 2300 gas and are considered safe against re-entrancy.
- B. .send throws an exception and .transfer returns a Boolean on error. Both just forward the gasstipend of 2300 gas and considered safe against re-entrancy
- C. .send returns a Boolean and .transfer throws an exception on error. .send is considered dangerous, because it sends all gas along, while .transfer only sends the gas stipend of 2300 gas along
- D. .send and .transfer are both considered low-level functions which are dangerous, because they send all gas along. It's better to use address.call.value>() to control the gas-amount.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 76**

All low-level functions on the address, so address.send(), address.call.valueQQ, address.callcode and address.delegatecall:

- A. are interrupting execution on error, because they throw an exception.
- B. continuing execution on error silently, which is the reason why they are so dangerous.
- C. returning Booleans to indicate an error during execution.
- D. .send() throws an exception, while the other functions are returning Booleans during execution to indicate an error.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 77** When using assert to check invariants and it evaluates to false:

- A. all gas is consumed.
- B. all remaining gas is returned.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 78** When using require to check input parameters and it evaluates to false:

- A. all gas is consumed
- B. all remaining gas is returned.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 79** To send ether to a contract without a function call:

- A. a fallback function must be declared and it must be made payable. If there is no fallback function or the fallback function is not payable it will throw an exception.
- B. either a fallback function which is payable exists, or no fallback function at all exists.
- C. you cannot send ether to a contract without explicitly calling a function. The fallback function can never receive ether.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 80** Using selfdestruct(beneficiary) with the beneficiary being a contract without a payable fallback function:

- A. will throw an exception, because the fallback function is non-payable and thus cannot receive ether.
- B. it's impossible to secure a contract against receiving ether, because selfdestruct will always send ether to the address in the argument. This is a design decision of the Ethereum platform.
- C. selfdestruct doesn't send anything to a contract, it just re-assigns the owner of the contract to a new person. Sending ether must be done outside of selfdestruct.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 81**

If you need more fine-grained functionality than solidity offers out of the box:

- A. you can incorporate inline-assembly to get better controls.
- B. you have to import pre-compiled assembly files which are then hard-copied into the bytecode of the compiled solidity file.
- C. you can use Viper, the experimental assembly like language specifically to offer more flexibility.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 82** Address.Call vs.

Address.Delegatecall:

- A. Address.call() is used for calling other contracts using the scope of the called contract in terms of storage variables. Address.delegatecall() is used for libraries, which uses the storage variables of the contract who called. Libraries are a great way to re-use already existing code and delegatecall can make sure that no storage is used from the library, instead it looks like the code is directly copied into the calling contract.
- B. Address.delegatecall() is used for calling other contracts using the scope of the called contract in terms of storage variables. Address.call() is used for libraries, which uses the storage variables of the contract who called. Libraries are a great way to re-use already existing code and call() can make sure that no storage is used from the library, instead it looks like the code is directly copied into the calling contract.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 83** It's not possible to use inheritance from multiple sources in Solidity.

- A. True
- B. False

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

Assert is used:

- A. to check internal states that should never happen.
- B. to check input arguments from users.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

.Require is used:

- A. to check internal states that should never happen.



B. to check input arguments from users.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

Truffle:

A. is a framework that helps developers with Testing, Deployment and Management of Smart Contracts and Distributed Applications.

B. is a library that helps developers to connect to Ethereum nodes, because it abstracts the JSONRPC interface.

C. is a framework for Java, similar to Web3.js for JavaScript. It's a great way to develop distributed Java enterprise applications.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 87** Unit-Testing on a local chain is important, because it helps you:

A. to run tests quickly and especially for free, compared to continuous deployment on the MainNetwork. This way you save a lot of fees, time and costs.

B. to run tests in an environment where logging is activated. On the Main-Net you have no access to transaction logs and this is ultimately the information you need to debug your contracts.

C. to avoid regression bugs with contracts that are updated constantly on the main-net. Once you update a contract on the main-net, the address stays the same, but the code changes and this can have disastrous side-effects.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88** It's easy to write clean-room unit-tests with truffle:

A. for Java, JavaScript, and C++

B. for JavaScript using Web3.js

C. for Solidity and JavaScript

D. for any language, as long as it adheres to the open Testing-Interface from Truffle

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 89** With the truffle config file you can manage:

A. the amount of gas your contract deployment and transactions, against your contract, will need. This way you can essentially lower the gas costs over traditional web3.js dApps.

B. different Networks to deploy your contracts to. This way you can easily deploy to a local blockchain, the main-net or the Ropsten/Rinkeby Test-Net with only one parameter.

C. you can manage your secret API keys to the Ethereum Network. This way you can get access to several different Ethereum nodes at the same time without the need to switch your keyfiles.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 90** Truffle boxes  
are a great way:

- A. to contribute to the box community which is the distributed file system for truffle.
- B. to start with a pre-configured environment for most web-development needs.
- C. to use tools that makes boxing of Dapps for different platforms very easy.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 91** Truffle has an integrated in-memory blockchain which makes unit-testing very easy:

- A. True, but it's still good to use Ganache, or even a real private network for testing.
- B. False, it's necessary to use Ganache or even a real private network for testing.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



**QUESTION 92** Using truffle-  
contract over Web3.js:

- A. is a must for every developer, because Web3.js changes so often.
- B. is a convenient way because Web3.js is currently still in beta and truffle-contract can handle transactions with JavaScript-promises.
- C. they are both completely different things. Truffle-Contract is a framework while Web3.js is a library.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 93** Why is Unit-  
Testing so important?

- A. It helps you to find bugs, regression bugs and sometimes also helps you to understand your code from different angles.
- B. It is a great way to spend time on something that you get paid for. But ultimately it will just slow down the development process.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 94** If you are starting a new ERC20 token:

- A. it would be best to start from scratch, just looking at the required interface.
- B. it is beneficial to copy and paste the already existing code from the Ethereum wiki and modify this until you like it.
- C. best is to start with an audited implementation, for example from OpenZeppelin, in order to reuse already existing code.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

To generate a random number:

- A. it's good to use the block timestamp, as this is always different.
- B. it's good to use the block hash as this is clearly always very different.
- C. it's good to use the RANDAO smart contract.
- D. it's not possible to have a random number in a deterministic environment such as the Ethereum blockchain.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 96** When you do external calls to other smart contracts:

- A. you should follow the checks-effects-interactions pattern and avoid state changes after the call.
- B. you should follow the effects-checks-interactions pattern and avoid state changes before the call.
- C. you should follow the checks-effects-interactions pattern, which is only necessary when you do calls to contracts where a direct contract call is not possible.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 97** When you are programming a game like poker or battleships where you need to hide opponents values is:

- A. with private state variables. This way nobody else other than the smart contract itself can see the information
- B. with external contracts holding those values. This way we can make sure that the information flow is following a clear logic and nobody else can access this information.
- C. You can't hide anything on the blockchain, because the information is public, just the call is private which means only other smart contracts would be limited in accessing that information.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 98**



When considering smart contracts and the blockchain it's good:

- A. to move all existing logic to the blockchain, so everything runs on the same system. This way it might be more complex, but easier to maintain.
- B. to move only those parts to the blockchain that really need the blockchain. This way smart contracts can be easier to read, easier to test and are not so complex.
- C. to move those parts to the blockchain that deal with Ether transfers. All other parts can remain in traditional database systems. This way only the value-transfer is on the blockchain.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 99** When a smart contract pays out money:

- A. it's good to use a push over a pull method.
- B. it's good to use a push and a pull method to ensure that participants can get their money no matter the contract state. In addition to and pushing it should contain a withdraw method.
- C. it's good to use only pull and no push method.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 100** To develop smart contracts:

- A. it's good to start with a local in-memory blockchain with unit tests but then deploy to the mainnet as rapidly as possible.
- B. it's good to start with a local in-memory blockchain with unit-tests. Then, in the next step, debug and test the smart contract on a test-net like Ropsten or Rinkeby with beta customers to iron out last issues before deploying it to the main-net.
- C. it's good to start with a test-net with beta-customers like on the Rinkeby or Ropsten testnet, before testing it locally on an in-memory blockchain simulation such as Ganache. Then deploy it to the main-net.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 101** To avoid issues during Ethereum platform upgrades:

- A. it's good to inform users about the updates via a newsletter.
- B. it's good to have the ability to pause a contract in order to manage the money at risk.
- C. Ethereum doesn't upgrade the platform. It's fixed and final.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 102**

Integrating the community into your testing:

- A. is great, because they often find bugs which weren't considered before.
- B. is not good, because you might give out secrets.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

