Mastering Blockchain – Review Questions

Welcome to the review questions for *Mastering Blockchain – Third Edition!* To provide an optional means of self-assessment, we have included five questions for each chapter, except the final chapter, which consists of ten questions. The questions will be made up of a combination of multiple choice questions, which will require you to select one or more answers as specified in the wording of the question, and longer, descriptive questions that require more detailed answers, based on what you have learned from the book.

We have produced questions based on core ideas—and their practical applications—from each chapter. All answers are based on the material from the book and the bonus online content; therefore, if you struggle with any questions you can always reread the relevant sections in the chapters to learn more about the topic. For each answer, we have also provided an explanation, which will help you to further augment your learning.

Please note that these questions are drawn from both the core book and the bonus online content.

Review questions

Chapter 1, Blockchain 101

1. What is a blockchain? Provide a definition in your own words.
2. Bitcoin can be defined as being which of the following terms?
    a. A blockchain
    b. A cryptocurrency
    c. A distributed ledger
    d. All of the above

3. The benefits of blockchain, as compared to traditional infrastructure services, include which of the following? Choose two answers.
    a. Decentralization
    b. Immutability
    c. Requirement of a trusted third party
    d. Scalability
4. What is a consensus mechanism? Provide a definition in your own words.
5. Define the CAP theorem and its three core properties.

Chapter 2, Decentralization

1. A blockchain's decentralized ecosystem mainly consists of which services? Pick as many answers as you think answer the question.
    a. Decentralized computation
    b. Decentralized storage
    c. Decentralized internet
    d. Decentralized communication
2. True or false: Ethereum is a platform originally designed to achieve and promote decentralization.
3. True or false: all distributed systems are decentralized.
4. Name the three scales of decentralization, and think of an example of each.
5. What does the Zooko's triangle concept require?

Chapter 3, Symmetric Cryptography

1. When is AES CTR used in the Ethereum networking stack?
    a. To encrypt the peer discovery process
    b. To encrypt **Directed Acyclic Graphs** (**DAGs**)
    c. To encrypt **Peer-to-Peer** (**P2P**) communications
    d. To encrypt smart contract code
2. What is confidentiality in the context of blockchain? Provide a definition in your own words.
3. What is non-repudiation in the context of blockchain? Provide a definition in your own words.
4. Define stream ciphers.
5. Define block ciphers.

Chapter 4, Public Key Cryptography

1. The RSA encryption algorithm is based on which problem?
    a. The integer factorization problem
    b. The discrete logarithm problem
    c. Zero-knowledge proofs
    d. None of the above
2. SECP256K1 is defined by which of the following terms? Choose two answers.
    a. Hash function
    b. Koblitz curve
    c. Domain parameters
    d. **Message Authentication Code** (**MAC**)
3. How does asymmetric cryptography differ from symmetric cryptography?
4. What are key establishment mechanisms used for in the context of information security?
5. What are hash functions used for?

Chapter 5, Consensus Algorithms

1. Consensus algorithms are designed to achieve which of the following properties in distributed systems? Choose two answers.
    a. Agreement
    b. Decentralization
    c. Liveness
    d. Asynchrony
2. Raft is which kind of protocol?
    a. A **Proof of Stake** (**PoS**) protocol
    b. A **Byzantine Fault Tolerant** (**BFT**) protocol
    c. A **Crash Fault Tolerant** (**CFT**) protocol
    d. None of the above
3. Partially synchronous consensus protocols rely on which of the following to fulfil the liveness property?
    a. Routing information protocols
    b. Timing assumptions
    c. Hash functions
    d. All of the above

4. HotStuff uses which of the following network topologies?
    a. Mesh topology
    b. Ring topology
    c. Star topology
    d. None of the above
5. What is an FLP impossibility result?

Chapter 6, Introducing Bitcoin

1. Bitcoin propagates network traffic using which of the following protocols?
    a. Bitcoin consensus protocol
    b. Gossip protocol
    c. SMTP
    d. None of the above
2. The block header in a Bitcoin block is how many bytes long?
    a. 120 bytes
    b. 180 bytes
    c. 80 bytes
    d. 60 bytes
3. A new Bitcoin block is created approximately every how many minutes?
    a. 1 minute
    b. 5 minutes
    c. 8 minutes
    d. 10 minutes
4. What is P2PKH?
5. Broadly describe the main stages of the Bitcoin transaction flow.

Chapter 7, Bitcoin Network and Payments

1. Which of the following is a commonly used hash function for Bloom filters?
    a. SHA1
    b. FNV
    c. MD5
    d. RC4

2. Deterministic wallets derive keys from which of the following values?
    a. Seed value
    b. Initialization hash
    c. Non-cryptographic hash function
    d. All of the above
3. How does the *headers first* block download approach work in Bitcoin's synchronization mechanism?
4. What is the `INV` network message used for in Bitcoin's block synchronization protocol?
5. The BIP70 payment protocol uses which type of certificate for authentication?

Chapter 8, Bitcoin Clients and APIs

1. The Bitcoin client's `regtest` mode is commonly used for which of the following processes?
    a. Mining with ASICs
    b. Creating local test blockchains
    c. Creating networks of nodes
    d. None of the above
2. Bitcoin configuration is stored in a file with which of the following names?
    a. `bitcoin.conf`
    b. `bitcoind.conf`
    c. `bitcoin.ini`
    d. `bitcoind.ini`
3. Which command-line tools can be used to interact with the JSON RPC API over HTTP?
    a. `netstat`
    b. `curl`
    c. `bitcoin`
    d. `finger`
4. Which of the following commands can be used to query the number of confirmations a block has received so far?
    a. `bitcoin-cli getblock`
    b. `bitcoin-cli getconfirmations`
    c. `bitcoin-cli gettransactioninfo`
    d. `bitcoin-cli getnetinfo`
5. Name the three methods of interacting with the blockchain using the Bitcoin client.

Chapter 9, Alternative Coins

1. Mixing protocols are used in blockchains to provide which of the following?
    a. Consensus
    b. Mining
    c. Access control
    d. Anonymity
2. Which of the following algorithm categories does DigiShield fit into?
    a. Consensus algorithms
    b. Difficulty adjustment algorithms
    c. Mining algorithms
    d. None of the above
3. Primecoin's **Proof of Work** (**PoW**) mechanism requires nodes to solve for which of the following in order to prove their commitment? Choose two answers.
    a. Factors of large primes
    b. Cunningham chains
    c. Bi-twin chains
    d. Large rational numbers
4. Zcash makes use of which of the following in order to provide privacy?
    a. Zk-SNARKs
    b. Zk-STARKs
    c. Zk-Rollups
    d. Concurrent zero-knowledge proofs
5. What are the main limitations of PoW mechanisms that have led to the development of other participation methods?

Chapter 10, Smart Contracts

1. Which of the following smart contract development languages is used in Ethereum?
    a. Solidity
    b. C
    c. Pascal
    d. Solidus
2. Define an oracle in your own words.

3. Reverse oracles are also known as which of the following?
    a. Outbound oracles
    b. Inbound oracles
    c. Multiplexed oracles
    d. None of the above
4. What three objects are Ricardian contracts made up of?
5. What is TLSNotary, and what is it used for? Provide a definition in your own words.

Chapter 11, Ethereum 101

1. Externally owned accounts, or EOAs, lack which of the following abilities?
    a. They cannot initiate a call message
    b. They cannot initiate a transaction message
    c. They cannot possess an ether balance
    d. All of the above
2. Code hashes in the account state are invoked via which of the following operations?
    a. Transaction calls
    b. Web3 calls
    c. Ether transfers
    d. Message calls
3. If the number of elements in the stack grows beyond 1024 during **Ethereum Virtual Machine** (**EVM**) execution, what happens to the EVM?
    a. It halts
    b. It restarts
    c. It jumps to the first instruction again
    d. None of the above
4. Broadly describe the process of key generation and address derivation in the context of the Ethereum blockchain.
5. What is RLP? Provide a definition in your own words.

Chapter 12, Further Ethereum

1. A block can be rejected if it has which of the following?
    a. A non-positive difficulty
    b. An invalid mix digest
    c. A duplicate uncle block
    d. Any of the above

2. Ethereum's PoW algorithm is called which of the following?
    a. DAG
    b. Ethash
    c. Equihash
    d. Nakamoto hash
3. What are the three synchronization modes in Ethereum's Geth client?
    a. Full, light, and none
    b. Complete, fast, and low frequency
    c. Full, fast, and light
    d. None of the above
4. The Geth client's keystore uses which type of cipher to encrypt keys?
    a. AES-128-CBC
    b. AES-256-CTR
    c. AES-128-CTR
    d. DES-128
5. What is the so-called "difficulty time-bomb" built into the Ethereum network, and what is its purpose?

Chapter 13, Ethereum Development Environment

1. The Goerli test network uses which of the following consensus algorithms?
    a. PoW
    b. **Proof of Authority** (**PoA**)
    c. PoS
    d. **Delegated PoS** (**DPoS**)
2. To encode a block in RLP, which of the following methods is used?
    a. `debug.getBlockRlp()`
    b. `eth.getBlockRlp()`
    c. `admin.getBlockRlp`
    d. None of the above
3. Which of the following objects does MetaMask inject into a browser?
    a. The Web3 object
    b. The Ethereum object
    c. The Solidity object
    d. All of the above

4. Which of the following commands can be used to list Ethereum accounts?
    a. `personal.allaccounts`
    b. `eth.accounts`
    c. `eth.allaccounts`
    d. `admin.ethaccountslist`
5. What is the `extraData` field used for in Ethereum's genesis configuration?

Chapter 14, Development Tools and Frameworks

1. Remix is a service that can be defined as which of the following?
    a. A compiler
    b. An IDE
    c. A coding language
    d. None of the above
2. External function calls in Solidity are made via which of the following?
    a. Transactions
    b. Calls
    c. Message calls
    d. None of the above
3. Exception handling in Solidity is provided by which function? Please choose as many options as you think answer the question.
    a. Assert
    b. Revert
    c. Pragma
    d. Require
4. What is Truffle and what can it be used for?
5. How are functions in Solidity identified at the time of execution?

Chapter 15, Introducing Web3

1. An ABI can be defined as which of the following?
    a. Automatic Binding Interface
    b. Application Binding Interface
    c. Application Binary Interface
    d. Application Base Interface

2. The Web3.js library is a collection of several modules that includes which of the following? Please choose as many options as you think answer the question.
    a. `Web3-eth`
    b. `Web3-interop`
    c. `Web3-utils`
    d. `web3-networks`
3. Which of the following commands is used to deploy smart contracts to the blockchain network in Truffle?
    a. `truffle deploy`
    b. `truffle init`
    c. `truffle migrate`
    d. `truffle upload`
4. The Web3 library allows interaction with Ethereum nodes using which protocols? Please choose as many options as you think answer the question.
    a. WebSockets
    b. HTTP
    c. IPC
    d. CORBA
5. Define Web3.js in your own words.

Chapter 16, Serenity

1. A validator is used to perform which of the following functions? Please choose two answers.
    a. Participate in Ethereum 2.0's consensus process
    b. Vote for new blocks
    c. Delete old blocks
    d. Perform Ethash
2. Which of the following key types does a validator hold?
    a. A signing key and a withdrawal key
    b. A slashing key and a deletion key
    c. A validation key and a wallet key
    d. All of the above

3. Phase 0 of the implementation of Ethereum 2.0 primarily involves creating which of the following?
    a. Shards
    b. The beacon chain
    c. Random oracles
    d. A new smart contract language
4. What is slashing, and what is its purpose on the Ethereum 2.0 beacon chain?
5. What is sharding in the context of Ethereum 2.0?

Chapter 17, Hyperledger

1. Hyperledger Fabric uses which of the following ordering services?
    a. SOLO
    b. Raft-based ordering service
    c. Kafka
    d. All of the above
2. Hyperledger Fabric's consensus mechanism works in steps. Which of the following processes accurately captures these steps?
    a. 1) Ordering 2) Endorsement 3) Commitment
    b. 1) Endorsement 2) Ordering 3) Commitment
    c. 1) Ordering 2) Commitment
    d. 1) Commitment 2) Endorsement
3. PoET consensus can be affected by two main problems. Which of the following options describes these problems?
    a. The stale chip and broken chip problems
    b. High electricity usage and a lengthy PoW process
    c. Timing issues and the dark oracle problem
    d. None of the above
4. Hyperledger Sawtooth supports which of the following processes?
    a. Parallel transaction execution
    b. Cross-chain token exchange
    c. Pluggable payment mechanisms
    d. Dynamic and pluggable consensus
5. In your own words, what is Hyperledger Caliper?

Chapter 18, Tokenization

1. Fungible tokens possess which of the following traits? Choose as many options as you think answer the question.
    a. Interchangeability
    b. Divisibility
    c. Indistinguishability
    d. All of the above
2. ERC-20 is a token standard that applies to which type of token?
    a. Fungible
    b. Non-fungible
    c. Non-transferable
    d. Restricted stake
3. In your own words, what is securitization?
4. What does the ERC-1404 standard allow for as compared to other ERC standards?
5. What are stable tokens in the context of blockchain? Provide a definition in your own words.

Chapter 19, Blockchain – Outside of Currencies

1. Adding a blockchain layer to the **Internet of Things** (**IoT**) architecture model in a blockchain-based IoT can provide which of the following?
    a. Consensus
    b. Decentralization
    c. **Machine-to-Machine** (**M2M**) communication
    d. All of the above
2. If an IoT device is resource-constrained, and therefore cannot run a local ledger or Geth instance, how can it access blockchain services?
    a. Using HTTP
    b. Using HTTP-RPC
    c. Using IPC
    d. Using data sharing
3. Describe the IoT network's five-layer architecture model.
4. How can a blockchain help simplify existing payment mechanisms?
5. What are the main applications of blockchain technology within the financial sector?

Chapter 20, Enterprise Blockchains

1. The fundamental requirements of an enterprise blockchain include which of the following?
    a. Decentralization, security, and public availability
    b. Performance, privacy, and access governance
    c. Performance, decentralization, and transparency
    d. None of the above
2. In **Blockchain as a Service** (**BaaS**), DApps are usually expected to be managed by which of the following entities?
    a. Enterprises themselves
    b. Cloud service providers
    c. Internet service providers
    d. None of the above
3. Quorum's privacy manager uses which of the following combinations of cryptographic primitives to provide transaction confidentiality?
    a. `CURVE25519`, `XSALSA20`, and `POLY1305`
    b. `SHA256`, `CURVE381`, and `BLS`
    c. `SALSA20`
    d. All of the above
4. What is TOGAF and what is it used for?
5. What are CorDApps, and how do they use flows to execute their functions?

Chapter 21, Scalability and Other Challenges

1. Attribute-based encryption is which type of encryption?
    a. Symmetric encryption
    b. Public key encryption
    c. Zero-knowledge encryption
    d. None of the above
2. Which of the following types of bug was exploited in the DAO hack?
    a. Retrievability bug
    b. Zero-knowledge bug
    c. Message log bug
    d. Reentrancy bug

3. Define anonymity, in the context of blockchain, in your own words.
4. How do **Invertible Bloom Lookup Tables** (**IBLTs**) help to achieve scalability and better performance in the Bitcoin network?
5. Describe what each of the following phases of model checking consists of:
    a. Modeling
    b. Specification
    c. Verification

Chapter 22, Current Landscape and What's Next

1. What is the key difference between **central bank digital currency** (**CBDC**) and cryptocurrency?
2. What can we assume DAOs will evolve into in the future, given the current advancement in AI and blockchain, and what may they be capable of on the blockchain?
3. What are ASBCs?
4. What is a potential way that illegal activity can be thwarted and monitored on the blockchain?
5. Which programming language does Kadena use for writing smart contracts?
    a. Pact
    b. Vyper
    c. Yul
    d. Solidus
6. Accounts in the EOS blockchain are represented by strings of which of the following lengths?
    a. 19 characters
    b. 9 characters
    c. 12 characters
    d. No limit
7. The EOS blockchain uses which of the following consensus mechanisms?
    a. PoW
    b. PoS
    c. Federated PoS
    d. None of the above

8. What is the name of the domain-specific language developed for writing smart contracts in Tezos?
    a. Solidity 2
    b. Black Swan
    c. Michelson
    d. Eureka
9. What is a sidechain, and what specific transfer process does it allow?
10. What do you think is the most promising future application of blockchain technology, and why?

Answers

Chapter 1, Blockchain 101

1. A blockchain is a type of distributed ledger. A couple of definitions are as follows:

    Layman's definition: A blockchain is an ever-growing, secure, shared record-keeping system in which each user of the data holds a copy of the records up to that point. These records can only be updated if all parties involved in a transaction agree to update them.

    Technical definition: A blockchain is a peer-to-peer distributed ledger. It is cryptographically secure, append-only, immutable, and updateable only via consensus or agreement among its current peers.
2. d. Bitcoin is a cryptocurrency, based on blockchain, which in turn comes under the broad category of distributed ledgers.
3. a and b. Decentralization and immutability, preventing alteration of records committed to the ledger, are two of the main benefits of a blockchain. Blockchain solutions actually remove the need of a trusted third party, and as yet, blockchains are generally not reliably scalable enough to call scalability a benefit.
4. A consensus mechanism is a set of defined steps that are taken by most or all nodes in a blockchain in order to agree on a proposed value. Consensus mechanisms have come into the limelight and gained considerable popularity with the advent of blockchain and Bitcoin.
5. The CAP theorem states that any distributed system cannot have the properties of consistency, availability, and partition tolerance simultaneously:
    a. *Consistency* is a property that ensures that all nodes in a distributed system have a single, current, and identical copy of the data.
    b. *Availability* means that the nodes in the system are up, accessible for use, and are accepting incoming requests and responding with data without any failures, as and when required. In other words, data is available at each node and the nodes are responding to requests.
    c. *Partition tolerance* ensures that if some nodes are unable to communicate with other nodes due to network failures, the distributed system continues to operate correctly.

Chapter 2, Decentralization

1. a, b, and d. In traditional services, computation, storage, and communication services are centralized in nature. With the use of blockchain technology, all these services can be decentralized. Internet access, however, is still a service provided by a central party.
2. True. One of the core values of the Ethereum platform is decentralization.
3. False. Not all distributed systems are decentralized, because even in a distributed system, where data and computation services are spread across multiple nodes in a network, there still exists a central authority (usually an administrator) that has control over all nodes and oversees processing services. This centralized command over the system makes the system centralized in nature.
4. The three scales of decentralization are fully centralized, semi-decentralized, and fully decentralized.

   Examples of each, respectively, include traditional banks as trusted third parties (fully centralized), competition-based cloud services provided by multiple vendors, where end users choose what level of service centralization suits their needs best (semi-decentralized), and finally, services with no central authority, such as Bitcoin (fully decentralized).
5. Zooko's triangle is a concept relevant to user identity that requires that the naming system in a network protocol be *secure*, *decentralized*, and *able to provide human-meaningful and memorable names* to the users. It is speculated that a system can have only two of these properties simultaneously.

Chapter 3, Symmetric Cryptography

1. c. Ethereum peers use AES in counter mode (AES CTR) to encrypt their P2P communications.
2. Confidentiality is the assurance that information is only available to authorized entities.
3. Non-repudiation is the assurance that an entity cannot deny a previous commitment or action by the provision of incontrovertible evidence. It is a security service that offers definitive proof that a particular activity has occurred.
4. Stream ciphers are encryption algorithms that apply encryption algorithms to plaintext using a keystream, on a bit-by-bit basis (one bit at a time).
5. Block ciphers are encryption algorithms that break up a plaintext message to be encrypted into blocks of a fixed length and apply the encryption block by block.

Chapter 4, Public Key Cryptography

1. a. RSA is based on the integer factorization problem, which is defined as decomposition of a composite number into a product of smaller integers. During the RSA process, the products of pairs of large prime numbers are used as composite numbers, which are computationally infeasible to factor, thus providing a one-way function that is required to build such cryptosystems.

2. b and c. SECP256K1 is a Koblitz curve, which is defined over $y^2 = x^3 + ax + b$. It also defines domain parameters of the elliptic curve in a standards document available here: `http://www.secg.org/sec2-v2.pdf`.
3. Asymmetric cryptography refers to a type of cryptography in which the key that is used to encrypt the data is different from the key that is used to decrypt the data. This is also known as public key cryptography.
4. Key establishment mechanisms are concerned with the design of protocols that allow for the setting up of keys over an insecure channel.
5. Hash functions are used to map arbitrarily sized data to fixed-length values. In other words, they are used to create fixed-length digests of arbitrarily long input strings.

Chapter 5, Consensus Algorithms

1. a and c. Decentralization and asynchrony are properties related to network governance and network type respectively, not consensus.
2. c. Raft is a CFT protocol. It cannot yet handle the presence of Byzantine faults in the network.
3. b. Making timing assumptions about messages passed in the network allows network progress, thereby achieving liveness even if the network is slower at times.
4. c. Star topology has been used in HotStuff to improve communication efficiency.
5. FLP impossibility states that there exists no deterministic protocol that solves consensus in a message-passing asynchronous system in which at most one process crash fails.

   Thus, an FLP impossibility result is one that due to even a single crash failure, the consensus process fails.

Chapter 6, Introducing Bitcoin

1. b. Bitcoin propagates network traffic using the gossip protocol, which spreads information in a P2P network by employing gossip-like phenomena similar to that in epidemic spreading and computer virus spreading.
2. c. The block header in a Bitcoin block is 80 bytes long.
3. d. It takes approximately 10 minutes to create a new Bitcoin block.
4. **P2PKH** (**Pay to Public Key Hash**) is the most commonly used transaction type in the Bitcoin network. It is used to send transactions to Bitcoin addresses. The format of the transaction is as follows:

```
ScriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
ScriptSig: <sig> <pubKey>
```

5. Bitcoin's transaction flow consists of the following stages:
    a. The sender creates and signs a transaction
    b. The transaction is validated and propagated on the network
    c. Miners pick up the transaction, create candidate blocks, and start mining
    d. The block for which the PoW is solved by a miner is considered "mined"
    e. The block is propagated and verified on the network, and the miner receives a reward

Chapter 7, Bitcoin Network and Payments

1. b. FNV functions are a special type of hash function that are suitable for use in Bloom filters due to their properties of speed and uniformity.
2. a. Deterministic wallets derive keys from a single starting point called a seed.
3. The core idea is that the new node first asks peers for block headers, and then validates them. Once this initial block header validation is completed, blocks are requested in parallel from all available peers. The parallel download is made possible because the blueprint of the complete chain is already downloaded in the form of the block header chain, and the only thing left to download is the actual block body, which can be downloaded in parallel.

    This means that instead of downloading all blocks sequentially one by one, the headers, which are smaller in size, are downloaded first, and then the bulk of the data (the block bodies) are downloaded in parallel. This results in a significant reduction in the time it takes to synchronize a new client with the blockchain.
4. The `INV` message is used by nodes to advertise their knowledge of blocks and transactions.
5. The BIP70 payment protocol uses X.509 certificates.

Chapter 8, Bitcoin Clients and APIs

1. b. `regtest` mode, or regression testing mode, creates a local test blockchain that can be used by developers for testing purposes.
2. a. Bitcoin client configuration is stored in a file named `bitcoin.conf`.
3. b. `curl` can be used to make requests over HTTP.
4. a. The number of confirmations a block has received so far can be found in the output of `bitcoin-cli getblock` where it shows `confirmations`.
5. Bitcoin CLI, the JSON RPC interface, and the HTTP REST interface

Chapter 9, Alternative Coins

1. d. Mixing protocols provide anonymity, usually by creating an anonymity set where 1 out of *n* possible elements is the real identity of a user.
2. b. DigiShield is a real-time difficulty adjustment algorithm used in cryptocurrencies such as Zcash.

3. b and c. While mining on the Primecoin network, nodes search for special prime number chains called Cunningham chains and bi-twin chains.
4. a. Zcash uses zero-knowledge Succinct Non-interactive ARguments of Knowledge, or zk-SNARKs.
5. The main limitations of PoW include the expense of mining hardware like ASICs, the mechanism's huge local and global resource and electricity usage, and its slow mining rate. PoS in particular is seen as a reasonable alternative to PoW due to PoS's lack of requirement of specialized hardware and (relatively) low energy consumption.

Chapter 10, Smart Contracts

1. a. Solidity is the primary language used in Ethereum for smart contract development.
2. An oracle is an interface that delivers data from an external source to a smart contract.
3. a. Outbound oracles take data from the blockchain and send it out to the external world.
4. A Ricardian contract can be represented as a tuple of three objects, namely *prose*, *parameters*, and *code*.

   Prose represents the legal contract in natural language; code represents the program that is a computer-understandable representation of legal prose; and parameters join the appropriate parts of the legal contract to the equivalent code.
5. The TLSNotary protocol provides a piece of irrefutable evidence to an auditor that specific web traffic has occurred between a client and a server. It is based on **Transport Layer Security** (**TLS**), which is a standard security mechanism enabling secure, bidirectional communication between hosts.

Chapter 11, Ethereum 101

1. a. EOAs cannot initiate a call; however, they can initiate a value transfer transaction and can have ether balance.
2. d. Message calls are used to invoke code hashes.
3. a. The EVM halts if the number of elements in the stack grows beyond 1024.
4. The process of key generation and address derivation is as follows:
   a. First, a private key (a 256-bit positive integer) is randomly chosen under the rules defined by the elliptic curve `secp256k1` specification (in the range `[1, secp256k1n - 1]`).
   b. The public key is then derived from this private key using the **Elliptic Curve Digital Signature Algorithm** (**ECDSA**) recovery function.
   c. An address is derived from the public key, specifically, from the rightmost 160 bits of the Keccak hash of the public key.

5. RLP is a specially developed encoding scheme that is used in Ethereum. Its purpose is to serialize binary data for storage or transmission over the network, and also to save the network state in a Patricia tree on storage media. It is a deterministic and consistent binary encoding scheme used to serialize objects on the Ethereum blockchain, including the account state, transactions, messages, and blocks. It operates on strings and lists to produce raw bytes that are suitable for storage and transmission. RLP is a minimalistic and simple-to-implement serialization format that does not define any data types and simply stores structures as nested arrays.

Chapter 12, Further Ethereum

1. d. A block in Ethereum is rejected if it has any one of the properties of non-positive difficulty, invalid mix digest, or duplicate uncle blocks.
2. d. Ethash is used as Ethereum's PoW algorithm.
3. c. The Geth client can work in three modes, full, fast, and light.
4. c. AES 128-bit in counter (CTR) mode is used to encrypt the keys in the keystore.
5. Ethereum's difficulty time-bomb is the plan for mining difficulty to gradually increase to the extent that it is eventually very difficult or impossible to mine on the PoW chain, which will force users to move to the PoS chain.

Chapter 13, Ethereum Development Environment

1. b. The PoA protocol, Clique, is used for consensus in the Ethereum blockchain's Goerli test network.
2. a. `debug.getblockrlp()`, which takes a block number as a parameter and returns the RLP-encoded output.
3. a. MetaMask injects the Web3 object into the browser, which exposes several methods to interact with the blockchain.
4. b. `eth.accounts` returns the list of addresses owned by the Ethereum client.
5. `extraData` is a parameter that allows a 32-bit arbitrary value to be saved with the block.

Chapter 14, Development Tools and Frameworks

1. b. Remix is an **Integrated Development Environment** (**IDE**) intended to make smart contract development easier, offering tools to compile, debug, and test code, and use many different plugins and other features available within the same environment.
2. c. Message calls are used to make external function calls in Solidity.
3. a, b, and d. Exception handling in Solidity is provided by the `assert`, `revert`, and `require` functions.
4. The official line from the Truffle website is "Truffle is a development environment, testing framework, and asset pipeline for Ethereum, aiming to make life as an Ethereum developer easier."

   A more simple description is that it is a development framework that makes the tasks of testing and deployment easier and more manageable for developers.

5. Functions in Solidity are identified by their signature, which is the first four bytes of the Keccak-256 hash of the full signature string.

Chapter 15, Introducing Web3

1. c. ABI stands for Application Binary Interface, which acts as an interface between the application and backend smart contract.
2. a and c. There are three modules in Web3.js, namely `web3-eth`, `web3-shh`, and `web3-utils`.
3. c. `truffle migrate` is used to deploy contracts to a blockchain network.
4. a, b, and c. Web3 can make use of WebSockets, HTTP, and IPC mechanisms to allow connectivity with the blockchain node (an Ethereum node).
5. Web3.js is a collection of libraries written in JavaScript that allows interaction with local or remote Ethereum nodes.

Chapter 16, Serenity

1. a and b. Validators are required to participate in the consensus process and vote for new blocks (attestation).
2. a. There are two types of key held by a validator node: a signing key and a withdrawal key. The signing key is used to sign the blocks, whereas the withdrawal key is used to withdraw funds.
3. b. Phase 0 of Ethereum 2.0 is focused on creating the beacon chain, which serves as a backbone for the entire Ethereum 2.0 ecosystem. This includes connectivity with the Ethereum 1.0 chain, shard chains, and execution environments.
4. Slashing is a mechanism to penalize the entities that deviate from the protocol and expected behavior on the network. The main purpose of slashing is to make it prohibitively expensive to attack Ethereum 2.0. Secondly, it forces validators to perform their duties.
5. Sharding introduces shard chains, which allow increased transaction throughput and immediate finality. The state of each shard chain will be written periodically to the beacon chain. This is called a crosslink, which is a set of signatures from a set of validators (the committee) that has attested to a block in a shard chain. This crosslink is included in the beacon chain representing the attestation of blocks of shard chains.

Chapter 17, Hyperledger

1. d. Hyperledger Fabric allows the use of SOLO, Raft-based, and Kafka ordering services.
2. b. First a transaction is endorsed, then it is ordered (using an ordering service), and finally it is committed.
3. a. PoET is affected first by the stale chip problem, where SGX-based hardware can be purchased excessively to gain an advantage in the PoET consensus mechanism. It is also affected by the broken chip problem, where if a hardware chip is compromised, it simply means that the PoET process is compromised and the malicious actor can win the right to block proposal every time.

4. a and d. Hyperledger Sawtooth supports parallel transaction execution and pluggable consensus.
5. Hyperledger Caliper is a benchmarking framework for blockchains. It can be used to test and report performance characteristics of a blockchain.

Chapter 18, Tokenization

1. d. Fungible tokens are interchangeable, divisible into fractional ownership, and indistinguishable from one another.
2. a. ERC-20 applies to fungible tokens.
3. Securitization is the process of creating a new security by transforming illiquid assets into tradeable financial instruments.
4. The ERC-1404 standard allows the issuance of tokens with regulatory transfer restrictions. These restrictions enable users to control the transfer of tokens in different ways.
5. Stable tokens or stable coins are a type of token that has its value pegged to another asset's value, such as a fiat currency or precious metal. Stable tokens maintain a stable price against the price of this asset.

Chapter 19, Blockchain – Outside of Currencies

1. d. A blockchain-based IoT can benefit from the consensus layer of the blockchain, which would allow the maintenance of consistency and integrity across the network.

   Moreover, decentralization being a fundamental trait of blockchain, IoT would benefit in requiring no central authority to control devices, relying instead on the network rules for governance.

   Blockchain will also allow secure M2M communication using the P2P network. Note that P2P can be achieved without blockchain, but with blockchain it is expected to be more secure, due to core blockchain attributes such as immutability and consensus.
2. b. Usually, a resource-constrained IoT device can access blockchain services using HTTP over RPC, where a remote Geth node can serve requests from the IoT device.
3. The IoT can be defined as a network of computationally intelligent physical objects (such as cars, fridges, and industrial sensors) that are capable of connecting to the internet. By doing so, they can sense, collect data react to real-world events or environments, and communicate data over the internet.

   A five-layer model can be used to describe this definition of IoT, which contains a physical object layer, a device layer, a network layer, a services layer, and an application layer. Each layer or level is responsible for various functions and includes multiple components.
4. Current payment systems are centralized and are governed by traditional financial service industry codes and practices. These systems work adequately, but with the advent of blockchain, the potential of technology to address some of the inherent limitations in this system has become clear, which would result in faster cross-border payments, decentralization, and security.

5. Some of the main applications of blockchain in the financial sector include simplifying payments, post-trade settlements, and enhancing **Know Your Customer** (**KYC**) and identity checks.

Chapter 20, Enterprise Blockchains

1. b. Enterprise blockchains first and foremost require a high level of performance, which fulfils the needs of enterprise settings. They also prioritize privacy, which primarily covers confidentiality and in some cases anonymity, and access governance, which provides control over who can join the network.
2. a. Enterprises or businesses using a BaaS solution will be provided with the infrastructure and software required to run the blockchain, but they usually run and manage their own DApps on the network.
3. a. `curve25519`, `xsalsa20`, and `poly1305` are used as authenticated encryption mechanisms to provide transaction confidentiality.
4. TOGAF, or The Open Group Architecture Framework, enables organizations to systematically design, plan, and implement enterprise blockchain solutions in businesses.
5. A CorDApp (Corda Distributed Application) is a distributed application that runs on a Corda network. It allows nodes on the network to reach an agreement regarding updates to the ledger. For this purpose, flows are defined that describe a routine for the node to execute.

Chapter 21, Scalability and Other Challenges

1. b. Attribute-based encryption is a type of public key cryptography that provides confidentiality and access control simultaneously.
2. d. The DAO hack exploited the reentrancy bug, which allows the repeated calling of a function without the completion of the previous execution.
3. In the context of blockchain, anonymity is concerned with hiding the sender or receiver's identity in a network. This is opposed to confidentiality, which is concerned with hiding the actual payload or transaction value of a transaction.
4. IBLTs were proposed to reduce the amount of data required to be transferred between Bitcoin nodes. The key attraction in this approach is that it does not result in a hard fork of Bitcoin if implemented. The idea is based on the fact that there is no need to transfer all transactions between nodes; instead, only those that are not already available in the transaction pool of the synchronizing node are transferred. This allows quicker transaction pool synchronization between nodes, thus increasing the overall scalability and speed of the Bitcoin network.
5. The process of model checking consists of the following steps:
    a. It starts with modeling, where a formal specification is created from an informal design of the model.
    b. The specification step comes next, where relevant properties of the design are specified using some logical formalism.

c. Finally, verification of the model is carried out, which checks all properties defined in the specification and provides results regarding the correctness of the specification. In case of false or negative outcomes, error traces with counterexamples are provided to help the designer to trace the error.

Chapter 22, Current Landscape and What's Next

1. The key difference between cryptocurrencies and CBDC is that CBDC is issued as money by a central bank as legal tender declared by a country's government. It is a digital form of fiat money, whereas cryptocurrency is more of a decentralized token of value that is not backed by government regulation, law, or any monetary body.
2. One thing that DAOs can be predicted to evolve into is artificially intelligent DAOs that will make rational decisions on behalf of humans on the blockchain.
3. ASBC stands for Application-Specific Blockchain. In an ASBC, a blockchain is specially developed from scratch for a specific application, or used only for a specific application, and is thus focused on a specific industry or business need.
4. One possible option is to have smart contract code scrutinized by government regulators, and to have only code that has passed strict government-mandated auditing executed on the blockchain. Furthermore, several data analysis techniques, potentially employing machine learning algorithms, could dig out patterns, leading to the actual source and destination of funds, in order to thwart any illegal activity.
5. a. The Pact language is a Turing-incomplete, safe, and performant programming language used on the Kadena chain.
6. c. EOS accounts are represented by a string limited to 12 characters that can only contain lowercase letters a to z and numbers 1 to 5.
7. d. EOS uses DPoS, where fewer nodes participate in consensus in order to gain a higher transaction throughput.
8. c. Michelson is a functional programming language that allows the development of smart contracts on the Tezos platform that are verifiable using formal methods.
9. A sidechain is a blockchain that runs in parallel with a main blockchain, which allows the transfer of value between them. This means that tokens from one blockchain can be used in the sidechain and vice versa. It is also called a pegged sidechain, because it supports two-way pegged assets.
10. One possible answer, in the author's opinion, is the convergence of different industries with blockchain, as well as the amalgamation of artificial intelligence, which will result in extremely exciting and groundbreaking applications.