Discussion Questions and Answers (Chapters 2–22)

Chapter 2 – History of Blockchain

(1) Define the three major characteristics of money that bitcoin possesses.

Bitcoin has three major characteristics of money. First, bitcoin is divisible similar to how fiat currency units are divisible into smaller units of previously existing units. The division takes place digitally in the form of bitcoin and other cryptocurrencies, but the divisibility still exists. Second, any medium of exchange (money) must also be useful as a unit of account, which bitcoin partially fulfills. Despite prior price volatility and continued lower levels of volatility, bitcoin has a value in other forms of currency. In fact, after the 2017 price bubble, volatility decreased substantially. Third, any medium of exchange must be portable. That is, it must be able to be transferred across borders and boundaries. As a digital medium of exchange, bitcoin is easily portable and can be transferred across borders without fees.

(2) Describe five core components of blockchain technology.

Blockchain technology has the following five core components that include but are not limited to the following. First, every blockchain has a tamper-resistant ledger, which is where the transactions and other information that have occurred on the blockchain network are stored. Second, this information stored on the ledger is approved, before posting on the network itself, via some sort of consensus methodology that enables network members to jointly confirm that data are presented correctly. Third, any blockchain is defined by the encryption protocols used to safeguard information, with the most famous iteration being the SHA-256 encryption protocol used by the bitcoin blockchain. Fourth, the management of this entire process (i.e., the way in which data are confirmed and added to the network itself) is generally managed by full nodes, playing an important role in maintaining the integrity of the blockchain network. Fifth, every blockchain is in some way defined by the peer-to-peer (P2P) nature of transactions that underpin the entire blockchain ecosystem, which greatly reduces the need for intermediaries and other third-party organizations.

(3) Define interoperability in the context of blockchain implementation.

In the context of blockchain implementation, interoperability equates

to how easily a blockchain network or application can transfer data among the blockchain platform and other technology applications. A blockchain is simply a record of transactions. For that information to be leveraged effectively, it must be able to be communicated effectively.

(4) Discuss how problems with scaling and interoperability affect wider blockchain utilization.

Issues involving interoperability and scaling are two major obstacles to wider enterprise or commercial adoption of blockchain technology. If blockchain cannot meet the needs of commercial business, both in terms of transaction processing and network capacity, or the ease with which data can be transferred between the blockchain and other technologies, implementation efforts are likely to fail. As efforts and other iterations of blockchain emerge, scaling and interoperability continue to come to the forefront.

(5) Describe how blockchain is helpful for e-commerce.

Blockchain and crypto assets, specifically stablecoins, can be helpful for e-commerce transactions. Such an arrangement mirrors many of the benefits and savings associated with other mobile and digital payment transactions. Venmo, PayPal, Square, and Zelle have capitalized on the growing need for digital and P2P payments, increasing demand for lower cost options and general dissatisfaction with traditional financial incumbents. Stablecoins and blockchain-based payment platforms are equally well positioned to take advantage of many of these market forces.

Chapter 3 – Review of Blockchain and Emerging Applications

(1) Explain what constitutes a blockchain network, including a main property of that network.

A blockchain network usually consists of specific agents with each transaction verified by an agreement among the majority of the agents. Unlike a traditional database, the data on the chain are permanently stored and cannot be erased once a transaction enters the system. To maintain a cumulatively added ledger in a blockchain network, cryptography is used to record transactions among the participating agents of the same network.

(2) List several differences between a public and a private blockchain.

The identities of users are anonymous in a public blockchain platform and known in a private blockchain platform. Relative to a private blockchain system, the speed of transactions is usually relatively slower in a public blockchain platform due to scalability. Transactions can be created by any participant in a public blockchain, but participation is limited to the members of a private blockchain platform. Despite these

expected differences, cases exist in which some of these properties are not always distinct between the two platforms.

(3) Identify two major benefits of using blockchain in supply chain management.

If blockchain is properly implemented, the origin of a problem item, such as a specific food if exposed to a bacteria, can easily be traced, and a corrective action can be made in that specific region. Without a blockchain system, the entire inventory for the same food throughout the chain, regardless where the contamination occurred, might have to be destroyed. In the case of supply chains using blockchain-based technology, the technology tracks goods and materials to prevent counterfeit products and low-quality products.

(4) Explain the concept of humans, technology, and organizations in the context of smart cities.

Blockchain systems encompass three interrelated factors of humans, technology, and organizations. The framework identifies the attributes of the sharing economy of a smart city. Thus, blockchain may influence and create value-added. Blockchain increases the accessibility and availability of technology, which makes people more willing to accept access over ownership and to trust organizations and technology.

(5) Identify some relatively news areas where blockchain might have applications.

Blockchain is relatively well-known to the financial sector, supply chain management, and the fields of accounting and auditing. Smart cities, water distribution, and waste management sectors are relatively new to this emerging technology. As the world's population increases, living conditions are likely to become more challenging in such areas as communication and access to resources. This change has brought about the emergence of smart cities. A smart city relies on innovation and technology to have something unique to offer, such as introducing smart parking or blockchain and Artificial intelligence (AI) into city life.

Chapter 4 – Technical Aspects of Blockchain

(1) Describe the concept of a block and its components.

A block is a main component in blockchain architecture. It is a kind of data structure to record transactions during a specific period. Once a block is completed and validated, it is a permanent storage that cannot be altered or removed. Blocks are connected with each other by a hashing code as a chain. A block consists of a header and transaction data. A header is section in a block that serves as a summary of data.

A header consists of several components such as version number, timestamp, difficulty target, nonce, previous hash, and Merkle root.

- *Version number* is the current version of the block structure. It is used for keeping track of changes and updating the block.
- *Timestamp* provides the time when the block is created.
- *Difficulty target* is a value used to show how hard is it to find a hash. It will be lower than the target defined by a system.
- *Nonce* is a random value that a miner is allowed to manipulate to get a block hash. Once it is discovered, then all transactions are added to the blockchain.
- *Previous hash* is the hash of the previous block. It is used for connecting with other block as a chain.
- *Merkle root* consists of all the hashes of all the transactions to form a single hash code.

(2) Identify two major properties of a blockchain network.

Two major properties of a blockchain network are decentralization and immutability.

- *Decentralization*: Blockchain is a distributed ledger that provides a way for data to be recorded and shared by multiple nodes or users. No single authority can approve the transactions or set specific rules for the delivery of data. So, blockchain is a decentralized system.
- *Immutability.* Blockchain introduces cryptographic hashing for enabling security in a block during the process of data transmission. It provides integrity in that blockchain data are difficult to alter or modify due to every chain being different. This property helps to prevent unauthorized access of data because an attacker would have to manipulate every single piece of the blockchain present on the network.

(3) Define a Merkle hash tree, describe its role in blockchain, and explain the meaning of a Merkle root in the block header.

A Merkle hash tree (MHT) is a hash-based data structure that efficiently organizes a large amount of data. It is a tree structure in which each leaf is a hash of a block and a root is the hash at the top. MHT is designed to verify the integrity of data stored in a node and transmitted between nodes in a P2P network. More specifically, MHT helps to ensure data remain in their original state without alterations or corrupted information. The Merkle root, which is the hash of all the hashes of all the transactions in the block, is a part of the block header. This scheme enables securely verifying that the network has accepted a transaction.

(4) Explain the meaning of a distributed ledger.

A centralized ledger has multiple ledgers, but only a master ledger keeps the true records as a clearinghouse. Unlike the centralized ledger, a distributed ledger has a single ledger that is shared by all nodes. All nodes have some level of access to that ledger and determine the ledger's true state. A distributed ledger in blockchain is a database that is distributed across several computers or nodes. Although a blockchain network is

physically located in different places, it has a single ledger that is shared by all nodes. A distributed ledger eliminates the need for a central authority or intermediary to process, validate, or authenticate transactions.

Chapter 5 – Public Blockchains

(1) Describe a public blockchain and mention three current applications.

A public blockchain is a permissionless blockchain, allowing universal access to read, write, and validate information stored in the network. Current applications of public blockchain are monetary and financial networks such as Bitcoin and Zcash, distributed computing and virtual machines such as Ethereum and EOSIO, and decentralized markets such as Sia.

(2) Explain how public blockchains ensure the adherence of transaction and block-writing rules.

Public blockchains ensure the adherence of transaction and block-writing rules through the consensus protocol. The consensus process goes beyond the rules that are written in the blockchain code and involves incentive mechanisms to ensure proper functioning of the validator network. The code sets the limit on miner activities that can be written into the software, for instance adding an invalid transaction (i.e., a transaction with insufficient funds or an incomplete executable contract), switching input or output addresses, or modifying transaction amounts. However, the code excludes all potential misbehavior such as rewriting a block already included on the blockchain, purposefully not including a transaction or writing empty blocks ("selfish mining"). These actions are regulated by explicit and implicit incentive mechanisms. An example of an explicit mechanism is the reward mechanism in Bitcoin, motivating but not imposing miners to write blocks following the most recently added block, as opposed to choosing a previous one. An example of an implicit mechanism is an agreement by miners not to mine on top of empty blocks, discouraging but not prohibiting adversarial miners from selfish mining.

(3) Discuss the need for predefined mechanisms and rules to modify a public blockchain's protocols.

Besides the straightforward need to fix errors in the code, blockchain protocols need to adapt to the evolving use cases, applications, technology, and overall characteristics of the blockchain ecosystem. Given the decentralized nature of public blockchains, no central authority is available to determine the need and to approve and implement changes in the protocol. These decisions are vested to the blockchain's community. However, the interests of different blockchain stakeholders might diverge, hence leading to potential conflicts. Predefined mechanisms and rules would allow potential users to make informed decisions and participate in the network

knowing beforehand the risks of future protocol changes. However, the permissionless nature of public blockchains also allows any user to replicate the blockchain and its protocols, modify them according to its own preference, and to launch an alternative blockchain, partly rendering the mechanisms and rules useless. Therefore, the existence of such mechanisms and rules is not a necessary condition for a public blockchain because even if present, it could be annulled by a hard fork on the blockchain.

(4) Proof of Work (PoW) consensus protocols have been criticized due to their high and continuously increasing mining cost. Discuss how mining cost affects the tamper resistance attribute of public blockchains.

In PoW consensus protocols, block-writing rights are pseudo-randomly assigned according to amount of resources such as energy, memory space, and elapsed processing time that a validator has contributed to the network. If an adversarial miner wanted to tamper with the blockchain by blocking transactions or deleting transactions, the miner would have to dedicate a substantial amount of resources to attain probabilistic control of the block-writing process (51 percent attack). Therefore, as the mining cost of a blockchain increases, the cost of attacking the blockchain also increases, hence reinforcing the blockchain's tamper resistance attribute.

(5) Discuss whether a public blockchain requires issuing its own native cryptocurrency to provide incentives to its validator network.

By creating its own native cryptocurrency, the blockchain network can reward validators for their contribution by issuing block rewards and transaction fees payable on such cryptocurrency. If this was not the case, validator's compensation would be limited to transaction fees paid by users through two alternative mechanisms, each with burdensome implications: (1) compensating validators through a nonblockchain ("off-chain") system or (2) compensating validators through a blockchain compatible external cryptocurrency (crosschain atomic swaps).

In both alternatives, blockchain users would require accepting some features present on the payment system or external blockchain, as well as losing noncompatible attributes. For example, both options would constrain blockchain transactions speeds to the transaction speed of the off-chain payment system or external blockchain. It would restrict the universe of potential users and validators to those individuals and institutions with access to the selected payment system. For the case of payments through traditional financial networks, it would most likely require eliminating the blockchain's anonymity and pseudonymity attributes since validators would need to be identifiable to receive payments.

(6) Describe the process of PoW.

PoW is the original consensus algorithm in the blockchain network. It is used to confirm transactions and create new blocks. It requires expensive computing power to solve a complex mathematical puzzle known as a PoW problem. The process of PoW is as follows.

- New transactions are broadcasted to miners in the blockchain network.
- With PoW, miners compete against each other to complete transactions on the network and get rewarded by solving a complex mathematical puzzle using a hashing algorithm.
- The first miner publishes the verified PoW with a fixed length input string to all other miners.
- Other miners apply it to the same hash formula to see if the outcome is the same.
- The validated transaction is requested to enter into a block.
- All participants in the blockchain network attempt to approve this validated transaction using a consensus algorithm. If a majority of the participants (i.e., 51 percent rule in bitcoin) agree, then validation of this transaction occurs.
- After a set of approved transactions is bundled in a block, this block is sent to all the participants (nodes) in the blockchain network.

Chapter 6 – Private and Hybrid Blockchains and Applications

(1) Differentiate between a public/permissionless and a private/permissioned blockchain.

Several core differences exist between a permissionless and permissioned blockchain. First, a permissionless blockchain generally has few, if any, barriers or restrictions as to what kind of individual can be a part of the network itself. Second, a permissioned blockchain may operate in a similar manner as a traditional enterprise database management system depending on the levels of restrictions and barriers to entry. Third, a blockchain's internal controls are simpler to establish in a manner conducive to enterprise adoption as a result of the increased permissions.

(2) List three advantages of a private/permissioned blockchain relative to a public/permissionless blockchain for enterprise usage.

Three advantages of a permissioned blockchain for enterprise usage are:

- Increased ease with which internal controls and access protocols can be constructed to safeguard the information and data stored and shared within this blockchain.
- Increased processing speed due to the fact that the consensus methodologies used at a permissioned blockchain need not be as complex or time consuming as those used at a permissionless blockchain.
- Enhanced opportunities for P2P activity because different network members can be granted different levels of access, custody, or control over the network information.

(3) Differentiate between stablecoins and decentralized cryptocurrencies.

Stablecoins differ from decentralized cryptocurrencies in several ways.

- A stablecoin is pegged, tethered, or otherwise connected to an external asset such as oil, gold, or other fiat currency.
- A single entity or small number of organizations generally issue and govern stablecoins.
- Although a firm limit might exist on the number of decentralized cryptocurrencies that can be issued, not every stablecoin operates in this manner.

(4) Discuss how CBDCs differ from other stablecoins.

A CBDC is a type of crypto asset that is governed and issued by a central bank or other type of quasi-governmental agency. The main difference between a CBDC and other stablecoins is that a governmental entity complete with the full backstopping of that governmental agency or count issues a CBDC instead a private sector organization. A CBDC may also not be based on any blockchain technology.

(5) Explain how consumer privacy is relevant to CBDCs.

A CBDC could allow a government to keep track of all transactions in which a user engages. As a result, a government could block anything it deems an undesirable purchase. A CBDC could also reduce tax evasion because users have minimal privacy. Additional factors related to consumer and institutional privacy are more closely connected to the potential for governments or governmental actors to potentially leverage CBDCs for surveillance purposes. Specifically, those involved in the CBDC development process need to guard against the potential for abuse, tracking, and targeting or certain individuals, institutions, or purchase types.

Chapter 7 – Consensus Mechanisms and Related Issues

(1) Discuss how Global Bling could adjust the amount of bitcoin that Vantage Mines paid for the diamond in Transaction #2 and whether it would belong to the same chain.

Any accounting correction, whether it be an adjustment (adding the difference as a new block) or deleting the transaction in a new block and subsequently rebilling it in yet another block (two new blocks), should be an additional transaction added to the same chain. A transaction that occurred earlier cannot be changed in that block, but amounts can be altered in subsequent blocks. This approach differs from traditional accounting systems where previous entries and financial reports can be adjusted.

(2) Explain whether the electrical energy and equipment costs required by PoW are justified.

The answer depends on the relation between the costs of PoW (e.g., energy, environment, equipment, and transaction latency) and its benefits (e.g., security, immutability, and protection due to its complexity). Using PoW cannot be determined on a "one-size-fits-all" basis. In some cases,

where immutability and security are quite important, the costs of PoW may be worth it. This situation could occur in real estate transactions, which do not occur often and where immutability of records is required. In other cases, such as many everyday retail transactions, PoW might be "too much" and not worth its costs in energy and equipment, given that thousands of transactions occur every minute. Banks most likely would prefer using a less robust mechanism for processing these types of payments, given that PoW can only handle a few transactions at any one time and each batch of transactions takes 10 minutes to process. However, since the network controls this 10 minute processing time, possibly this restriction could be modified. In summary, cost justification for using PoW is unique for each situation or context.

(3) Explain what is likely to happen to the PoW mining industry after the most recent halving of bitcoin.

Because mining is a business, any mining concern would need to examine its costs of operation and expected profit. With the block reward being halved in May 2020, a mining operation should be assessing whether its equipment is working efficiently and whether its power source is too expensive. Miners might cease mining if the equipment and energy costs are too high, given the current reduced payment. What was profitable yesterday might not be profitable today. Some expect a reduction in the number of miners as those who cannot remain profitable with the new pricing scheme are likely to quit. Ultimately, fewer miners could lead to a reduced hash rate and subsequently reduced energy requirements. Yet, having fewer independent miners could also lead to a greater centralization by a few mining pools.

(4) Discuss whether business owners are likely to be comfortable with a Proof-of-Stake (PoS) blockchain.

Since PoS is a mechanism of trust, where participants assume that the validator's own best interest is that of maintaining the chain and not conducting an attack, many businesses might be uncomfortable with this arrangement.

What is interesting is that Ethereum, which sponsors many smart contracts, is considering PoS as its mechanism in the future, but has yet to do so. As was seen with some of the potential attacks of PoS, attacks could occur if the attack or fork seems to be more profitable for the validator. Businesses are rightfully concerned by this naiveté of trust in PoS that could expose it to these types of attacks. On the other hand, PoS does not carry the high energy and equipment requirements of PoW, and blocks are validated more quickly. Similar to the analysis of PoW, in the end the choice to use PoS is context- and use-specific. In short, no single, definitive answer is available.

(5) Discuss whether the SHA-256 hash is appropriate for most blockchains.

SHA256 hashing is the fundamental technology proposed by Nakamoto. The complexity of hashing imparts the features of security,

immutability, and tamper resistance to bitcoin and other blockchains using PoW. However, these beneficial features come with a huge cost of equipment, substantial demands of energy, slow transaction processing, and concerns about mining centralization. The blockchain envisioned by Nakamoto and which currently exists as bitcoin seems to be irrelevant for today's potential uses. Businesses should be concerned about the financial viability of SHA256 hash based blockchains. Conversely, the blockchain might not be so secure or tamper resistant without hashing. Also, whether the chain could still be called a blockchain without SHA256 is unclear. At least, it would not be the bitcoin ledger that Nakamoto proposed. Clearly, the appropriateness of hashing as the proper consensus mechanism for a blockchain is context-specific and where the business carefully identifies the most important features for its blockchain transactions.

Chapter 8 – Token Economies

(1) Define a cryptographic token.

A cryptographic token is blockchain-native asset that facilitates new value creation and exchange models. It can represent a wide range of programmable assets or access rights managed by a smart contract and an underlying blockchain.

(2) Characterize Web 3.0 and identify the attributes that differentiate it from Web 2.0.

Web 3.0 is the decentralized web underpinned by public blockchain networks that eliminate the need for trusted third parties and proprietary protocols. At its core, Web 3.0 disintermediates economic transactions and enables users to assume self-sovereignty over their data and digital identity. With the introduction of a universal state layer, Web 3.0 is a major step evolution over Web 2.0. This state layer gives users a way to hold state (economic value) in a digitally native way and transfer it to anyone on the network, enabling truly P2P transactions without intermediaries. Web 3.0 is considered the internet of value.

(3) Define a utility token and indicate how it differs from a SoV/MoE token.

A utility token provides holders with access to a digital product or service and derive its value from this underlying right. It represents crypto asset that is intrinsic to the blockchain and inherently consumptive in nature. A utility token is designed to be used or consumed in the process. Although utility tokens can be traded among ecosystem participants, unlike SoV/MoE tokens, utility tokens are not typically used as a store of value (e.g., digital gold) or medium of exchange (e.g., for payments). They are typically developed for use within a decentralized application (dApp) that resides on top of an existing public blockchain

network like Ethereum. Several types of utility tokens exist including governance, discount, work, and burn-and-mint tokens.

(4) Explain the difference between fungible and nonfungible tokens and identify the appropriate Ethereum token standards for each.

Fungible tokens are identical in value, and they are interchangeable. The most common technical standard used for creating Ethereum-based fungible tokens is the ERC-20 (Ethereum Request for Comment 20) token standard. Nonfungible tokens (NFTs) represent something unique, can differ in value, and are noninterchangeable due to their individual distinct attributes. A common technical standard used for creating unique Ethereum-based NFTs is the ERC-721 token standard. The ERC-721 standard further extends the possibilities of fungible ERC-20 tokens with a higher degree of functionality, particularly around token creation and ownership. Crypto collectibles are typically created using ERC-721 NFTs.

(5) Explain why mechanism design is a critical component of cryptoeconomic systems.

Cryptoeconomic systems rely on incentive mechanisms to drive user behaviors in a way that creates a self-sustaining system. Token economies (i.e., complex token systems) are cryptoeconomic systems where individual actions that advance a collective goal are incentivized through the token. The incentive mechanism driving the interactions (i.e., token transactions) among actors (i.e., humans or autonomous agents) is an integral cryptoeconomic component of the token system. Mechanism design focuses on the development of effective cryptoeconomic incentives such that if actors pursue their own self-interests, they are simultaneously incentivized to reach the collective system-level goal – a win-win outcome. The cryptoeconomic incentive mechanisms can be engineered to encourage only those behaviors that contribute to the overarching goals of the token system as a whole, while disincentivizing destructive behaviors.

(6) Discuss how system dynamics modeling is useful to token engineering.

A general goal of all token systems is to create a coordinated outcome that satisfies system-level (i.e., global) goals. In reality, they can produce predictable (deterministic) but also unpredictable (stochastic) outcomes. Stochastic outcomes are often linked to human actors that do not always act in rational ways; they may be influenced by externalities that cause them to prefer actions other than those a model assumes. System dynamics modeling may help to demonstrate how a complex system behaves as a whole given varying assumptions about actor/agent behaviors. It can be a powerful tool to model the architecture of a token system visually using, for example, stock-and-flow diagrams. System dynamics models can help in exploring possible futures by asking "what-if" questions and simulating interactions between agents/actors to observe which macroscale effects emerge. Different simulations can be run in tools such as cadCAD (an open-source Python package) to help answer the "what-if" questions including Monte Carlo methods, A/B testing, and parameter sweeping.

Chapter 9 – Proposed Modifications to Spur Consumer Adoption of Blockchain

(1) Explain smart contracts and their use in blockchain.

Smart contracts are codes that are built into the software to act as law in the network. The smart contract design currently has flaws including errors in code but should eventually ensure that the law cannot be violated because it is built directly in the software and is not open to human interpretation. Once the code is ready to be used, exceptions to the contract are prohibited. Contracts currently used have loopholes because they can be interpreted in different ways. However, with a smart contract, the terms of the contract are absolute with little room for interpretation. This feature allows the government to have some control over blockchain's use so that the intended uses follow the current set of values and laws. For instance, blockchain can be programmed to record asset sales but only the assets that the government deems legal and for sale.

(2) Provide three reasons for why blockchain is an improvement to the current system of data security and data transfer.

Below are three reasons for why blockchain offers improvements over the current system:

- Blockchain can improve efficiency. It can save time because information is available to an individual thus avoiding waiting for a third-party response.
- Blockchain can lower costs. It can remove fees that someone has to pay to find necessary information. Thus, this information is readily available to the parties involved without waiting for a third-party response.
- Information is safer and better protected because fewer opportunities exist for it to be leaked or hacked. Decentralizing the data makes data more secure. Changes to data are also more transparent because a mandatory record of change is required.

(3) Discuss how blockchain may change the current view of accounting data.

Instead of seeing just what was exchanged in the transaction, the user can also see the cryptographic signature corresponding to the transaction. This feature gives the stakeholder a more accurate and transparent view of how the business is working and doing financially. The advancement into blockchain also allows for outside stakeholders or auditors to access a company's data easier and more securely.

(4) Identify the steps needed for blockchain to be effective.

The most important step for blockchain to be effective is to have more people adopt and start using it. Blocks are built off existing blocks, and as blockchain becomes standardized, acceptance across businesses is likely to increase. As more companies use blockchain, it can become more secure. In order for consumers to use blockchain, the government and private

businesses need to adopt the system. Once the government begins using blockchain for security of voting, using the Voatz application, or in the healthcare field, using MedRec, consumers must establish their identity on the blockchain. Establishing a person's identity on the blockchain becomes more necessary as private businesses use blockchain to monitor and record sales data. Once consumers are established on the blockchain, using OneName, the system is likely to become more effective. As identities and blocks are verified, chains can be established. As more chains are established, the PoW needed to verify if a block can be obtained from other verified blocks making the chains more reliable. Consumers are likely to find that as businesses use blockchain, it becomes more secure and efficient as well as less costly to participate in the blockchain system.

(5) Provide an example of how blockchain can benefit consumers.

Below are several examples of how blockchain can benefit consumers:

- Blockchain enables consumers to more easily and accurately prove ownership rights of contracts and intangible assets such as patents.
- Blockchain can create a P2P economy where more people can participate in buying and selling of data or products without waiting for or relying on intermediaries such as retailers.
- Patients can access health records through MedRec, which allows them to view their entire medical history and any amendments to it.

Chapter 10 – Blockchain: Speed, Efficiency, Decreased Costs, and Technical Challenges

(1) Describe the business use cases related to blockchain traceability and transparency.

Some of the business-specific benefits and opportunities related to blockchain technology involve the traceability and transparency that a blockchain network can deliver to network members. Specifically, the ability to trace, monitor, and report on the whereabouts of pieces of physical goods or information on a continuous basis is likely a benefit for almost every organization. Food safety, healthcare information, and the ability to more closely monitor supply chains on a global basis are a few that increased traceability can be of benefit. Additionally, the transparency inherent to any blockchain platform, via the access that members have to network data, allows more comprehensive and real-time analysis. That is, the combination of traceability and transparency allows making better analysis and taking more proactive business actions.

(2) Discuss how blockchain implementation may decrease costs among network partners.

Several ways are available in which blockchain implementation may reduce costs among network members. Since network members are

allowed access to a shared ledger of information that is up-to-date as the information changes, less need exists for manual confirmations and verifications. Other potential benefits include lower auditing and accounting costs as information is updated on a more frequent basis. Insurance claims and the processing of those claims can occur on a more real-time basis, reducing the time and expense of waiting for claims to be processed and ultimately paid out. Lastly, the billions in fees and other costs commonly associated with transferring financial information can be reduced as a result of blockchain implementation, generating savings that flow directly to the bottom line.

(3) Describe how interoperability issues can complicate blockchain implementation.

Interoperability is the way in which blockchain can communicate with other blockchains and other technology systems. The true value of any information or data management system is the efficiencies and analyses that can be conducted as a result of sharing that information. A lack of standardized methods by which blockchains can interoperate with other blockchain and technology systems hinders achieving blockchain's benefits. That is, interoperability may represent one of the largest obstacles toward enterprise adoption, as the sharing and free flow of data underpin many of the savings and benefits linked to blockchain implementation.

(4) Explain how a lack of blockchain standards impede wider adoption of blockchain technology and platforms.

Perhaps, the single largest impediment to wider commercial adoption of blockchain technology is the lack of standards for how blockchains should be regulated and incorporated into existing regulatory frameworks and structures. Blockchain is a technology tool and platform. For any technology tool to become widespread within the business landscape requires clear, consistent, and enforceable standards. Since blockchain platforms can store and transfer large amounts of potentially proprietary information, ensuring industry and blockchain specific standards for controlling access to information is essential.

Chapter 11 – The Importance of Interoperability, Decentralization, and Choice

(1) Discuss the importance of decentralization for achieving interoperability.

The development of the early internet provides some valuable lessons for the maturity of the blockchain ecosystem.

Whenever a gap occurs in interoperability, the private sector would forego decentralization and the free flow of information for commercialization and profits. The blockchain ecosystem developed without interoperability in mind in a race to be the most secure, cheapest, and fastest blockchain.

That ecosystem is playing catch up with some amazing innovations for crosschain compatibility among many others, but the question whether blockchain will end up in the same place as the "balkanization of the internet." Blockchain has consistently delivered choice, for example, by allowing users to secure their own crypto assets or using a custodian for storage. It may not be a centralized versus decentralized winner take all scenario after all, but rather a blockchain ecosystem that allows users to choose which way they want to work while having full transparency and disclosure about the networks and data they are using.

(2) Discuss another level of interoperability beyond interopchains.

Both Polkadot and Cosmos achieve high levels of interoperability by creating the internet of blockchains albeit by different approaches. Cosmos connects a more varied set of independent sovereign blockchains that are responsible for their own security while Polkadot centralizes security into a single relay chain by forgoing the sovereignty proposition. These two examples indicate how different alternative approaches could emerge. Assume four interopchains with unique value propositions that are akin to super clusters in the universe example. Interoperability still needs to be present among the interopchains, so the super clusters form the universe – the internet of blockchains. One blockchain could simultaneously reside in multiple interopchains at the same time, thus, creating full connectedness.

(3) Explain whether sidechains need to be interoperable.

Sidechains create interoperability between their corresponding primary chains. The main purposes of sidechains are to provide more features than a primary chain, accelerate development, and reduce risk of introducing new features on a primary chain. Sidechains create a lower level of interoperability than interopchains but nonetheless provide important on-ramps and off-ramps. If sidechains were connected with interopchains, a native token like bitcoin could be used with an almost unlimited set of features and the ability to swap with any other token to be used with any dApp.

(4) Discuss the importance of oracles for supplying data to blockchains and how they create interoperability.

Smart contracts depend on off-chain data to execute as designed on predefined parameters. Although not all smart contracts require off-chain, enterprise adoption and business use will not happen without oracles. A decentralized network is only as decentralized as its most centralized part. If off-chain data such as weather information, crop yields, and election results feed smart contracts from a centralized source, a single point of failure undermines the entire value proposition. Otherwise, centralized data sources have to be transformed into decentralized data to proclaim a fully decentralized system. Therefore, robust oracles could be the most important domain in the coalescence of the internet of blockchains.

Chapter 12 – Convergence with Artificial Intelligence and Other Related Concepts

(1) Identify the two branches of AI research and the branch more relevant to blockchain.

The branches of AI research are deductive inference methods with logic inference and inductive inference methods with learning from past data. The current mainstream AI applications are based on inductive inference methods. They mimic human decisions based on past data. Although inductive inference AI cannot understand how to make such a decision using past human decision data, it can still replace manual intervention in many situations as long as they can make a similar decision as the past human decision. As a relatively new technique to share data across multiorganizations, blockchain is more relevant to inductive inference AI methods.

(2) Identify the techniques that serve as the foundation for the current mainstream AI applications.

Since the current mainstream AI applications are data driven, foundation techniques are related to data in both hardware and software. Hardware techniques involve data capture, storage, and computing; software techniques deal with how to analyze data to provide business insights.

(3) Specify three data analytical methods and how they relate to each other.

Three types of data analytical methods are descriptive analytics, predictive analytics, and prescriptive analytics. Descriptive analytics summarizes patterns from past data. With summarized patterns, predictive analytics use them to predict the future based on the assumption that historical patterns repeat themselves. With forecasted results from predictive analytics, prescriptive analytics uses them to identify the optimal plan to meet a future need.

(4) Discuss how blockchain can be integrated with AI applications.

Blockchain is a relatively new technique to share data across multiorganizations. It provides the opportunity for AI applications to improve the collaboration across multiorganizations. Also, blockchain can ensure data completeness, accuracy, and consistency, which help AI methods to make more accurate inferences based on better quality data.

Chapter 13 – Risk Management and Transference Issues in Blockchain Technologies

(1) Discuss how cryptocurrencies are classified by the various government entities described in the reading.

The Commodity Futures Trading Commission may consider virtual currencies to be commodities. The Internal Revenue Service treats virtual currencies as property. According to the Securities and Exchange Commission, cryptocurrencies may circumstantially be deemed

securities. Courts may or may not consider cryptocurrencies to be "quasi-tangible property." Thus, no coherent classification system currently exists across the various government entities.

(2) Explain whether a standard commercial crime policy affords coverage to a business for blockchain breaches and cryptocurrency losses.

Commercial crime policies are unlikely to afford coverage for blockchain-related losses due to the common definitions found within these policies. Losses for certain cryptocurrencies may be circumstantially covered if the policy language is amended as necessary to cover direct or indirect losses.

(3) Explain whether a standard commercial general liability policy affords coverage to a business for blockchain breaches and cryptocurrency losses.

Although a cryptocurrency may be considered "quasi-tangible property," common Coverage A exclusions often rule out electronic data as "not tangible property." These exclusions would likely also eliminate coverage for any blockchain-related losses. Coverage B exclusions are likely to explicitly prohibit any coverage for the breach of sensitive information as personal or advertising injuries. Circumstantially, Coverage B may offer some protection from class action lawsuits following a breach, though this protection is likely to depend on the fact pattern of the breach and allegation presented by the plaintiffs. Coverage C generally covers medical payments associated with bodily injury and rejects coverage of blockchain or cryptocurrency losses.

(4) Explain whether a standard cyber insurance policy affords coverage to a business for blockchain breaches and cryptocurrency losses.

The main hurdle to establishing coverage under a cyber insurance policy for blockchain losses centers on the notion of "custody and control." Consortium, public, and many types of private blockchains that include multiple parties eschew the traditional notion of custody and control that is relied upon for cyber insurance policies to trigger coverage. Coverage for cryptocurrency-related losses may be covered either by definition or through an endorsement.

(5) Identify the alternative insurance mechanisms available for businesses.

The various alternative insurance mechanisms available include self-insurance mechanisms or captive insurance for blockchain losses. Certain companies are now offering standalone insurance policies for cryptocurrency losses.

(6) Discuss the various attacks of vectors and vulnerabilities that may be present in blockchains.

The listed methods include: key attack, identity attack, manipulation attack, service attack, malware attack, application attack, reputation attack, and quantum attack.

- A *key attack* occurs when vulnerabilities or "backdoors" occur in the cryptographic standards being used.

- An *identity attack* occurs when a third party uses various means to compromise the identity of the blockchain user.
- A *manipulation attack* centers around one or modes of the network being fully or partially removed to allow for further exploits.
- A *service attack* can take many forms. One prominent example of a service attack is a distributed denial of service (DDoS) attack. In a DDoS attack, unknowingly infected computers from third parties are used to flood the network to inhibit legitimate transactions.
- A *malware attack* occurs when mining software is surreptitiously installed in an unknowing victim's computer to enable the third party to gather cryptocurrency from other's efforts. Cryptojacking is one example of a malware attack.
- An *application attack* is particularly pernicious because it focuses on the application that interacts with the blockchain to steal funds.
- A *reputation-based* attack can either be accomplished by creating new accounts or hiding negative transactions. The goal is to fool the framework into believing that a dishonest user is a new and honest participant.
- A *quantum attack*, though currently hypothetical, focuses on using the power of quantum computers to "break" encryption algorithms. These algorithms are effectively unbreakable through brute force attacks with the calculation speeds of current computers.

Chapter 14 – Legal and Regulatory Issues in the Temporary Regime

(1) Explain how the Securities and Exchange Commission (SEC) came to be the primary regulator of alt-currency and blockchain.

The SEC dominance in this field arose both by consumer involvement and regulatory default. The Treasury Department and the Internal Revenue Service withheld classification of cryptocurrency while concurrently millions of "investors" purchased shares of companies designed to trade cryptocurrencies or the digital assets themselves. The larger question may be whether Congress and/or the States are likely to ultimately overtake the SEC as the primary regulator in the field. For the time being, SEC rulemaking seems inevitable.

(2) Explain the legal authorities supporting the application of American securities law to alt-currency and blockchain.

The SEC uses the *Howey* test to classify purchases as agreements known as "investment contracts" under the securities laws. In turn, the Department of Justice and private plaintiffs have employed the same legal rationale to a successful end. In sum, the four factors of the test seek answers to these questions:

- Has there been an investment of money?

- Was there a "common enterprise" between issuer and investor(s)?
- Did the investor have an expectation of profit?
- Did the enterprise depend upon the essential managerial efforts being expended by the issuer?

If all four questions can be answered affirmatively, a security is present, and the securities laws apply regardless of the title given to the deal or transaction, or the intentions of the parties to subject the deal to the securities laws.

(3) Identify the criticisms of the SEC's rapid and expansive reach.

Critics express several concerns about the SEC's rapid and expansive research. First, no Congressional statute or even SEC Rule authority exists for extending jurisdiction over digital asset instruments. Second, discord exits at the Commissioner level over the proper approach to regulation. Third, not all crypto deals lend themselves to traditional securities analysis. Noteworthy distinctions concern the consideration exchanged for digital coins, the use of digital coins within a contained environment, and the lack of any intent by the ICO issuer to encourage third-party speculation.

(4) Discuss noteworthy state initiatives to bring cryptocurrency transactions and blockchain technology within traditional means of regulation.

In terms of a uniform "code" capable of being adopted by the States, progress has stalled in that fewer than a dozen States appear to be interested in contemplating the adoption of a uniform measure. In terms of individual State approaches, responses vary. Some States merely echo the view of the Treasury Department that money transmitter regulations may apply. Others such as New Jersey have encouraged the virtual currency business by adopting statutes bestowing tax benefits. At the other end of the spectrum, a few States have imposed "bitlicense" requirements obligation businesses that trade in cryptocurrency to register and adhere to compliance obligations such as recordkeeping and net capital minimums. New York has enacted the strictest of such regulations.

(5) Discuss the most immediate regulatory change that is expected.

SEC rulemaking is the likely next step. The TurnKey No Action Letter, while only actually being binding on one party, provides insight into the rationale behind any eventual agency rule. The four factors highlighted by this publicized guidance appear to be the following:

- The degree to which the issuer was already capitalized,
- The avoidance of statements leading investors to believe in a third-party market for the trading of such tokens,
- The efforts to create a limited environment for using the digital token, and
- The valuing of the digital coin at "par" (i.e., at nominal or face value, as opposed to a value set by the market).

Chapter 15 – Regulatory Ambiguity and Its Impact on Blockchain

(1) Discuss whether the treatment for cryptocurrencies is consistent among various US regulators.

US regulators treat and interpret cryptocurrencies in different ways. For example, the IRS treats cryptocurrencies as property while other regulators such as the Commodities Futures and Exchange Commission (CFTC) and SEC treat them as commodities and/or securities in some cases.

(2) Explain how cryptocurrencies are taxed in the United States.

According to Notice 2014–21, cryptocurrencies are treated as "property" by the IRS. Therefore, all the general rules applicable to property apply to cryptocurrency-related transactions. According to this logic, an investor who holds cryptocurrency as a capital asset could experience capital gains and capital losses. Calculating the gain or loss amount involves determining the difference between the sales price and the cost basis of the crypto asset.

(3) Discuss how staking rewards should be taxed.

Notice 2014–21 does not directly address staking. However, the guidelines for mining activity suggest that staking rewards should be taxed at the time of the receipt. However, what type of income staking rewards constitute is unclear. One view is that staking generates a type of rental income because the taxpayer is lending a "property" and receiving rewards.

(4) Indicate how the IRS is trying to increase cryptocurrency tax compliance.

The biggest initiative the IRS took recently to increase compliance was to include a question on cryptocurrency on Schedule 1 of the tax form stating "At any time during 2019, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency?" Every US taxpayer has to answer this question going forward. The IRS believes including such a question is likely to lead to higher voluntary compliance.

Chapter 16 – Considerations for Blockchain Adoption and Integration

(1) Identify and discuss the attributes of blockchain technology that add value as a technology-based system but also require the implementation team to make special considerations during implementation.

Some attributes of blockchain technology adding value to an organization as a technology-based system include decentralization, synchronization, traceable, immutability, security, scalability, auditability, and programmability. These attributes also mean that an organization must make special considerations during the implementation phase. Below are some questions that need to be addressed during implementation.

- *Decentralization*: In many blockchain implementations, an organization's data may be stored outside of its existing facilities and relies on encryption to protect it from cybersecurity threats. Has the organization made efforts to address the legal, hardware, software, and personnel requirements to assure that the data are safe and the organization is protected in case of a breach?
- *Synchronization*: Have procedures been put in place that assure that when new nodes are added to the network that the data are accurately synchronized, and the new node adds to the network's functionality?
- *Traceability*: Since each transaction can be traced back to its authors and the nodes performing the validation, has the organization considered how it can identify these nodes and authors so that actions can be taken if necessary?
- *Immutability*: The immutable nature of blockchain eliminates the ability to remove data if necessary or even preferred. Is the organization prepared to have data out on a public blockchain that may have been created in error but still remains immutable? Has the organization considered the internal challenges that this situation may produce?
- *Security*: The primary value of keeping an organization's data in plain sight depends on its security features using SHA-256 encryption for each block of data in the chain. How has the organization prepared to test the proper functionality of these security features to demonstrate to its customers and investors that its data are secure?
- *Scalability*: Adding new nodes on a private or public network enables scalability. What has the organization done to assure that when new nodes are added from new outside providers that these providers are working for the organization and are not nefarious actors who have an interest in the organization's data?
- *Auditability*: An attractive attribute of blockchain in that the date, time, smart contract details, and the various node activities are all recorded and immutable. Has the organization considered how this type of data can coexist with its current internal processes such as private transactions or operations and activities that receive a top secret or confidential classification?
- *Programmability*: Blockchain uses smart contracts, which are custom programs written by skilled personnel to emulate the details of how the organization does business. For example, if the process to close on a deal between two parties contains the fields or attributes date, time, party 1, party 2, amount from party one, amount from party 2, and text-based specifics of the deal, then a small program or smart contract would need to be created to make sure that contract was added to the blockchain properly each time that type of transaction was processed. Is the organization prepared with skilled personnel? Has it considered all processes within the organization that require a smart contract?

(2) Discuss the various costs involved with implementing a blockchain solution within an organization.

When implementing blockchain, an organization must consider both initial and recurring costs associated with hardware, software, data conversion, and programming, adapting internal procedures and processes, and recruiting and retaining quality personnel. As the organization begins the planning phase after deciding to implement a blockchain solution, cost considerations should be a main focal point in the planning.

With the implementation of a pioneering technology, the proper skilled personnel are often expensive and in short supply. Three areas with the highest paid technology personnel are data science, programming, and cybersecurity. Blockchain requires experts in all three areas. How has the organization prepared for these personnel requirements?

(3) Discuss the technical and organizational capabilities that an organization should examine before venturing into a blockchain implementation.

Before undertaking a blockchain implementation, an organization should consider such factors as short- and long-term personnel requirements, budgetary planning to determine the total cost of ownership of the new system, the risks faced if the implementation fails, and its ability to reach its target return on investment from the system implementation. Although an organization may decide to implement a blockchain solution for many reasons, it must assure that the implementation adds value that exceeds the forecasted costs of implementing and maintaining the network. How has the organization identified its current status and capabilities to successfully implement the new technology? What preparations must it make to successfully implement and maintain the blockchain solution?

(4) Discuss why an organization might decide to implement a blockchain solution.

An organization might decide to implement a blockchain solution to meet standards set by industry regulatory agencies, to be competitive in its market space, or to prepare for a world that is likely to be run on a blockchain system. The following provides a discussion of these reasons:

- *Meet regulatory standards*: An organization that is required to meet certain security requirements for its data such as Health Insurance Portability and Accountability Act (HIPAA) of 1996 or Sarbanes–Oxley Act of 2002 may decide to implement a blockchain solution to secure its sensitive data and eliminate the fines associated with repetitive breaches and loss of data. In this case, the organization must plan for the potential loss of data from the internal processing system or enterprise resource planning (ERP) system that prepares the data to be added to the blockchain. How has the organization prepared to secure both systems?

- *Gain a competitive edge*: If an agency has chosen to implement blockchain to gain a competitive edge over their competition, how will the organization market its new blockchain solution to its customers and investors? If customers are still going to see a forward facing website interface, how will they know their data are more secure than the organizations competitors?
- *Prepare for a blockchain world*: Depending upon the industry that the organization is servicing, management needs to determine whether a transition to blockchain technology as the primary driver of vendor selection by their target markets is likely to occur. If this case occurs, then the organization may decide to implement a limited blockchain solution involving its key operating systems. Taking this action is likely to help the organization identify any major obstacles when the time comes to fully implement a blockchain solution to stay competitive.

(5) Explain technological challenges that an organization may face when implementing a blockchain solution.

When implementing blockchain, an organization may encounter challenges involving system throughput, system latency, data size and system bandwidth, system scalability, data malleability, transaction authentication, and system security. Once an organization decides to implement a blockchain solution, it then selects a blockchain model (private/public), a technology platform, acquires and configures the necessary dedicated hardware and software, creates smart contracts, begins entering transactional data, and tests the entire system for performance and validity. At some point, it activates the blockchain system as part of its regular operating systems.

Implementing a proven technology is more straightforward and more predictable than blockchain. With blockchain, implementers need to consider challenges to the technology functionality and efficiency. For example, if each transaction takes 10 minutes to validate and is available to the blockchain users, how has the organization prepared to adjust to these delays? If it selects a public blockchain model and allows external miners to validate their data, how has the organization prepared to vet and qualify these miners to assure its customers data are secure?

Chapter 17 – Blockchain Applications in Finance

(1) Discuss the common uses for blockchain within financial services.

The most direct use cases of blockchain within financial services rest largely within the improvement and optimization of operational processes by having a shared and trusted source of important data. As in the case of FX and shareholder voting, the technology seeks to reduce counterparty touchpoints and provide greater transparency to the ecosystem's

members. The technology also aims to reduce the costs associated with recordkeeping.

(2) Describe the current system of shareholder voting and how blockchain may improve the process.

Shares are currently voted by electronic or paper means. Shares are held with the DTC on behalf of participants, which include banks, brokers, and other intermediaries acting on behalf of the underlying beneficial owner. The multiple layers of ownership obfuscate who the beneficial owner is because the DTC considers the shares to be owned by the depositing institution. Nonvoted shares for most matters are allowed to be voted by the record owner beginning 10 days before a shareholder meeting, even without direct permission from the record owner. Blockchain can bring greater transparency regarding the true ownership of shares, as owners have their own keys to verify who they are and what they own. Furthermore, the immutability of the blockchain can be a deterrent for bad actors and is likely to optimize and provide clarity around the tabulation and confirmation process.

(3) Explain how blockchain can help optimize post-trade FX operations.

Blockchain allows participants both internally and externally to better track the process of post-trade activities. Permissioned parties can track the information on the ledger at all times. Specifically, blockchain could make the trading netting process more efficient as the decentralization of data across multiple internal parties provides greater clarity on an institution's net exposure. This distributive factor would remove the redundancy of paperwork between different segments of the institution that accumulates while ensuring information is uniform and correct.

(4) Give some reasons a single enterprise might find effectively implementing a blockchain solution difficult.

The DLT is specifically designed to place data into the hands of multiple and sometimes competing participants. To assure that all parties trust the data, many copies are stored in the network, and new data must receive the approval by a majority of the participants. A blockchain owned by a single enterprise would likely have fewer copies. The company could be biased in approving data that serves its own interests, rather than the composite interests of a collective of participants. Thus, the blockchain may fail to be a trusted source of transaction data.

(5) Identify several benefits that might be derived when multiple companies in a line of business, like insurance or utilities, and its regulators share a blockchain.

Competitors in a line of business often need to cooperate. For example, they may agree on standards of technology, so interoperability of products would exist across vendors. By pooling data in a blockchain, competing companies can share data about common regulations that all must follow and identify potential frauds or other hazards that affect all companies. By

sharing the data in a blockchain, they assure that the data are mutually trustworthy because they all adhere to the constructs of DLT.

(6) Identify several applications for a blockchain whose ledger stores the sales of homes in a region.

By having sales data of homes available to various participants in the real estate industry, such as brokers, lenders, and title insurance companies, the potential exists for providing reliable pricing data for both buyers and sellers, clear and trusted transfer of ownership of a property, and the ability to find the best terms for securing a loan or choosing a broker.

Chapter 18 – Blockchain Applications in Healthcare

(1) Explain under which conditions compliance with the HIPAA in the United States and General Data Protection Regulation (GDPR) in the European Union with respect to the healthcare data management can be waived.

Neither HIPAA nor GDPR govern the use or disclosure of deidentified health information because deidentified (anonymized) health information is no longer considered protected health information. Automatic deidentification approaches can be applied for faster deidentification and can also be used with large data volumes. If proved that the desired anonymity level is achieved, requirements of HIPAA and GDPR can be waived.

(2) Discuss the purposes of ecosystems for health information exchanges (HIEs) and their limitations.

The creation of ecosystems for HIEs occurred to ensure that the patient data from electronic health records can be shared nationwide securely, efficiently, and accurately. HIEs have limited adoption, and many regional networks are still isolated from each other. Current implementations lack standard architecture resulting in a failure to ensure proper security level and enforced access control over shared patients' data. HIEs are generally designed as a single fully trusted entity solely responsible for managing and storing EHR data from multiple participating hospitals.

A centralized system suffers from a single point of failure threat and can become a performance bottleneck for real-world deployment. Additionally, a centralized authority having access to sensitive health information has more security and privacy concerns from the users. Alternatively, all the data can be stored and managed in the encrypted form, which can be problematic in medical settings. Often, a need exists to access and analyze all historical data including images in plain for better healthcare decisions.

(3) Identify major application areas in healthcare where blockchain technology can be employed and the main advantages of using blockchain in these areas.

A growing number of existing blockchain technology implementations reveals multiple advantages of using this new technology in

different aspects of healthcare. Blockchain can be used in primary care to achieve patient-centric data management while ensuring the patient's privacy and advancing personalized medicine; in connected health and pharmaceutical supply chain by bringing optimization of various healthcare processes, especially when multiple stakeholders are involved; and in medical research to ensure compliance to accelerate clinical studies.

(4) Explain how the immutability property of blockchain can contradict existing regulations in healthcare and the approaches used to achieve compliance with "the right to be forgotten."

According to the GDPR in Europe, a patient has "the right to be forgotten." This right to erase the data cannot be easily compatible with the immutability property of most blockchain technology implementations. However, applying different cryptographic techniques such as asymmetric encryption, threshold encryption, and proxy re-encryption could be used to address such limitations.

Another approach is to use so-called redactable blockchains. To generate the block identifier, redactable blockchains use a specific type of hash functions ("chameleon" hashing), employing a "trapdoor," which is a secret parameter that allows to find collisions. One can change the content of a block or remove blocks without the need to integrate the change in all the consequently added blocks on the ledger. One or multiple users possessing the secret parameter can make this change. Therefore, the policy regulating the access to the trapdoor is critical in such blockchain-based systems.

(5) List the barriers to adopting blockchain-based systems in healthcare.

Adopting blockchain-based systems in healthcare faces the following barriers:

- Technical barriers and limitations of current implementations: These barriers include difficulties when managing identities, credentials, lifecycle of the keys; a limited number of transactions per second, amount and structure of the data that can be stored on blockchain and efficiently retrieved; and the impossibility of relying on a single peer for a query about the state.
- Potential single point of failure when using permissioned blockchain technologies.
- Verification of the smart-contracts design and implementation.
- Definition of unified rules for the global reachability of the data including the usability and education for the patients on how to define access-control policy and what are the consequences of data-sharing decisions.
- Creation of robust and secure "break-glass" mechanisms for emergency situations.

- Ensuring compliance with regulations, including HIPAA in United States and GDPR in Europe.

Chapter 19 – Blockchain Applications in Real Estate

(1) Discuss the concept of proving (verifying) real estate ownership.

Ownership is proved or verified by examining the chain of the title including all previous records to corroborate the entity or the person claiming ownership. The goal is to ensure a valid claim and possible limitations to which such a claim may be subject. This process involves examining the linkage of each transfer document in the public record to confirm a proper link is evident and without defect. Further, this process would uncover any liens, mortgages, easements, or other claims against the property that may still be unsettled and, thus, eliminating doubt about the title for the party claiming ownership. This entry record is known as a chain of title. Attorneys, title searchers, and/or title abstractors normally carry out the process as part of the normal transactional closing and often in conjunction with the issuance of a title issued by a title insurance company.

(2) Identify a major challenge for using blockchain in real estate.

The largest major challenge to using blockchain in real estate is the lack of a unified and consistent real property database among different users and organizations. Records of ownership and encumbrances are most often held at the local county or municipality level and subject to multiple local and state laws as well as differing local standards of practices. Further, not all of these databases are digitized and rarely even standardized county to county in the same state. Establishing a required unified real property record database with all parcel, owner, and encumbrance information would make blockchain applications challenging. Yet, the task of gathering and standardizing the data should not be insurmountable.

(3) Explain debt financing for transactions in real estate.

Debt financing for real estate usually comes in the form of mortgage loans from commercial banks or government-backed lenders who issue debt to finance a purchase or refinance a transaction in exchange for a promissory note and lien against the property. The lien, or mortgage, allows the lender to reclaim ownership of the real property in the event of default through a process known as foreclosure. The combination of personal liability and security interest in the real property allows mortgage loans to routinely cover at least 80 percent of the total value of property being transacted. As such, the mortgage industry is critical and integral in the overall real estate system. From the perspective of a bank (lender), a mortgage is classified as a secured asset.

(4) Explain the use of blockchain in mortgage servicing.

Mortgage servicing is a procedure for managing the processing of payments and all other related tasks required to administer the loan after it is originated and closed. In normal operations, mortgage servicing involves receiving payments from the borrower and paying the net proceeds to the loan's owner, monitoring for compliance or payment from escrow all property taxes and property insurance bills, and ensuring the loan is fully paid off before releasing the security document. When loan default occurs, the servicer must manage the process until resolution of default or foreclosure. Further, the servicer must manage the transfer of servicing rights and ownership of the loan, which can occur frequently in secondary trading.

(5) Indicate how blockchain may reduce the challenge of maintaining and monitoring the physical conditions of a real estate property.

A blockchain could enable communication among parties and monitoring of the physical property by owners or managers, who may be located in different cities or even countries, by using smart sensors, smart contracts, and other blockchain-enabled applications that are linked to the physical property. Such communication would enhance or supplement the monitoring by onsite property management, which can be difficult from distances. As an example, a smart sensor in an elevator or a HVAC system could record cumulatively all maintenance activities to a blockchain that the owner or property manager could review to ensure the maintenance staff is conducting scheduled preventative maintenance.

Chapter 20 – Blockchain Applications in Supply Chain

(1) Describe permissioned blockchains and discuss why they should be the type of blockchain to adopt in the supply chain context.

Permissioned blockchain, as opposed to public blockchain, is a private blockchain available only to the members of that blockchain. Adding new members requires a permission process from the existing members. For a supply chain, since members of the supply chain share much confidential information related to supply chain transactions as well as proprietary and contracts related data, the information stored in the blockchain must be private and confidential to the members of the supply chain. Therefore, in this context, the blockchain must be permissioned rather than public.

(2) Explain how a blockchain enabled supply chain creates advantages for providing better product tracing, reducing counterfeiting, and eliminating shipping trade partners, and intermediaries.

Since information about orders and their associated transactions are maintained on a shared and distributed ledger system in the blockchain, all of these data can be traced to any point in the supply chain. Therefore, any

product-related information can be traced back to the point of origin of those data.

Counterfeiting is a major problem in supply chains. Currently, on a disconnected system, replacing a genuine product or component with a counterfeit product or component is easy because other companies in the chain would have difficulty becoming aware of it. Usually, other companies learn about such information much later if an issue arises with the product functionality or safety due to the counterfeit component. A blockchain reduces and in many cases eliminates this possibility because information related to a component or product must be appended to the block. Companies know that the data on the blockchain are irrefutable, so a single company cannot replace a genuine component with a counterfeit equivalent. Furthermore, sharing data may actually deter counterfeiting.

Much of the shipping logistics involves trade and shipping intermediaries and paper-based/manual processing. Blockchain provides a potential for not requiring these intermediaries since a seamless supply chain could eliminate the need for them.

(3) Discuss the possible developments in adopting blockchain for the global logistics industry.

A broad network of companies may want to form a permissioned blockchain where all entities required for the logistic operations could be part of the blockchain. This network could include shipping ports, freight carriers, road transport companies, government agencies, and insurance firms. Some examples are TradeLens and GSBN. Other similar blockchains could possibly evolve as more companies adopt the technology for global logistics.

(4) Discuss if and how companies can leverage existing technologies when implementing a blockchain platform.

Since the 2000s, companies have made substantial investments in RFID and ERP systems. Companies looking at blockchain would want these existing technologies to work on the blockchain platform. RFID information can be stored on the distributed ledger. ERP system data can be interfaced with the shared system to push or pull data from the intracompany ERP to the interorganization blockchain.

(5) Identify potential issues that companies face with smart contracts in the supply chain.

Smart contracts and their capability of triggering automated payments based on a completed transaction from sourcing to delivery are attractive aspects of implementing blockchain. Reducing the overall cash conversion cycle and lead times are also possible through this mechanism. However, some doubts exist if these changes could be done in a completely automated manner. Companies also need to address potential contract law and compliance issues before these changes become a reality.

Chapter 21 – Crypto Accounting, Valuation, Reporting, and Disclosure

(1) Explain the primary differences between decentralized cryptocurrencies and stablecoins or otherwise more centralized crypto assets.

Three primary differences exist between decentralized cryptocurrencies and stablecoins.

- Decentralized cryptocurrencies are not connected to any underlying asset whereas stablecoins are.
- Stablecoins can at least theoretically be redeemed or otherwise exchanged for the underlying physical asset, which could possibly add to the accounting and reporting considerations.
- Stablecoins are purported to be a fiat alternative and should operate as such. To do so, a clear mechanism must be available for redeemability or being used as a fit alternative.

(2) Discuss the disclosure implications around crypto assets, smart contracts, and blockchain control issues.

The reporting and disclosure requirements around smart contracts and other crypto assets remain an evolving issue that requires further analysis and consideration. Full transparency and disclosure appear a logical course of action moving forward, including a more robust dialog around the reporting of these crypto assets for both financial and operational reporting.

For some of the specific issues connected to crypto-asset reporting, several considerations take a primary role. First, where should crypto assets be disclosed on the financial statements? Should disclosure include valuation methodologies? How are changes in valuation reflected on the financial statements? Second, what reporting requirements and attestation practices should be integrated into financial audits and reporting as a result of smart contract development? What role should internal audits and information technology professionals play versus external auditors, and what impact is this role likely to have on SOC engagements? Third, will the P2P nature of transactions being processed and reported affect the reporting of information to the marketplace? Much like how XBRL information influenced SEC disclosures, will blockchain change the pace with which information pertinent to crypto assets and smart contracts is reported?

Authoritative answers in 2020 are difficult to come by due to the lack of consistent authoritative guidance, but several specific statements can be made. Auditors and attestation professionals will need to collaborate with regulators and enterprises to develop appropriate and robust standards and best practices. SOC engagements and financial statement audits will need to evolve to incorporate and integrate blockchain into how these engagements are carried out in terms of disclosure, audit findings, and reporting

expectations. Additionally, reporting and disclosing blockchain-specific information will become increasingly standardized and consistent as adoption continues to accelerate moving forward. Lastly, the potential development of more centrally managed crypto assets – be they issued by a government, a single entity, or a consortium of organizations – seems positioned to accelerate the improvement of reporting and disclosure standards.

(3) Discuss how the lack of valuation guidance can provide a headwind or obstacle to broader crypto asset adoption.

Lacking guidance, the marketplace is seeking a solution to address the issues and considerations involving the reporting, valuation, and disclosure connected to crypto assets. The lack of guidance and authoritative standards has resulted in multiple white papers and other publications but without any single institution being able to claim an authoritative position. The result of this situation remains to be seen, but the plethora of documentation is likely to result in debates and conversations connected to this issue until a time that authoritative guidance emerges.

(4) Identify how a lack of consistent accounting guidance and frameworks for crypto assets might cause confusion on the part of external users.

Investors and other market actors largely rely on the production and dissemination of consistent and comparable information. Without such guidelines, investors and other associated counterparties face difficulty in properly evaluating, reporting, and disclosing information connected to crypto assets. A major obstacle to broader and wider adoption of crypto assets is the lack of regulation and guidelines connected to how these assets should be reported, which is exacerbated by the patchwork approach that seems to be emerging.

(5) Explain how an auditor might go about incorporating a smart contract into an existing audit process.

An auditor might need to account for two key factors when incorporating a smart contract into a traditional audit. First, control testing needs to be increased. Clarification is needed on who has access to the blockchain and information stored therein, and how these blockchains are updated over time. Additionally, control testing over how blockchains interoperate with existing technology platforms needs to evolve, specifically involving how wallets and smart contracts are integrated into the organization. Second, the function of audit and attestation professionals must evolve and change. Rather than focusing only on verifying the information reported by management teams and how blockchain changes the processing and recording of transactions, audit, and attestation professionals should be able to assess both business and accounting objectives. For example, as larger entities such as Wal-Mart and JP Morgan continue to implement permissioned blockchains, the importance of being able to implement and maintain manual controls to

offset potential errors and omissions that could result from automation increases. This importance and role applies to different size organizations as many suppliers and partners who are not developing the blockchain become integrated within the platform. Smart contracts provide the technology by which blockchains can communicate with other blockchains and other technology applications. Thus, smart contracts play a critical role in the future of the audit and attestation process.

Chapter 22 – Auditing and Examining Blockchain Information

(1) Discuss how the audit of information stored on a blockchain differs from traditional audit information systems.

Audits of information stored on a blockchain differ from traditional accounting information systems because the blockchain contains external evidence validated by third parties, which may eventually reduce the need for current audit practices and evidence gathering activities. Traditional accounting information systems are centralized and managed by the entity under audit. With blockchain, the information is distributed and generally each node to the system takes part in the validation, lessening the risk that fraudulent or fictitious entries are validated on the blockchain and entered into the financial statements.

(2) Identify the internal control objectives that are specific to audits relying on information stored on the blockchain.

The audit of internal controls over financial reporting for information on a blockchain requires the auditor to understand the internal control environment, access permissions, consensus determinants, and smart contract implementation. Blockchains are only as strong as the weakest node the blockchain so auditors must verify that companies using blockchain for financial reporting have strong governance and controls in place to admit new nodes and for the validation of transactions. Auditors must also verify that access and validation controls are designed and operating effectively.

(3) Discuss the challenges of auditing digital assets.

Digital assets require the auditor to validate the current price and validate rights. Validating prices is challenging because of the numerous digital asset exchanges, with many offering similar cryptocurrencies for different prices. Auditors must determine the main market or most advantageous market from various potential markets. Auditors must also verify that holders of digital assets have legal rights, custody, and physical access to their assets. Digital assets are often stored on blockchain with encrypted access codes managed by a selected few individuals or entities. Auditors must verify that controls are in place for the owner to access and possess the assets if necessary.

(4) Explain how blockchains can improve the quality of auditing and assurance services.

Blockchains can improve the quality of audit work by providing higher quality evidence in a single location – the blockchain. Auditors can access this information through a client's portal or even as a node to the blockchain. This access allows auditors to spend less time focusing on evidence gathering activities for more routine transactions and more time on areas of the audit that require judgment and professional skepticism – audits of estimates and complex and/or nonroutine transactions.

(5) Explain how blockchain can change the way audit and other assurance services are provided.

As blockchain continues to move audits toward a more controls-based audit, emphasis is likely to be placed on the design and operation of controls for clients using blockchain for financial reporting purposes. Blockchains require assurance providers to understand and review complex coding and automatic controls and auditors to better understand interconnected reporting systems across multiple nodes.