Public and Private Ledgers

LATEST SUBMISSION GRADE

90%

1. How does ownership attribution on a public blockchain differ from that of a private blockchain? **1 / 1 point**

- (●) On a public blockchain, ownership of an asset is attributed to an address, which is pseudonymous. On a private blockchain, ownership attribution may or may not be pseudonymous; the identity setup is a design decision.
- ( ) On a public blockchain, ownership of an asset is attributed to a self-selected username, which may or may not be pseudonymous. On a private blockchain, ownership attribution is indicated using a company's ticker symbol.
- ( ) On both public and private blockchains, ownership of an asset is attributed to a private key. On a public blockchain, private keys remain hidden from the network, whereas on a private blockchain, companies must disclose their private keys as part of their reporting requirements.
- ( ) None of the above

✓ **Correct**
The identity setup of a private or consortium blockchain is a design choice.

2. What is a key difference between a centralized and distributed ledger? **1 / 1 point**

- ( ) A centralized ledger can be backed-up, whereas a distributed ledger cannot.
- ( ) A centralized ledger is more resilient to hardware failure compared to a distributed ledger.
- ( ) In a centralized ledger all data is stored in a single location, whereas in a distributed ledger fragments of the full dataset are spread across across multiple locations.
- (●) A centralized ledger is controlled by a single, highly-trusted entity, whereas a distributed ledger is controlled by multiple, independent nodes who each retain a full copy of the ledger.

✓ **Correct**
In a distributed ledger, control is distributed amongst the nodes in the network.

3. Which of the following best describes a **public** blockchain? **1 / 1 point**

- ( ) Anyone can view the ledger.

- ○ Anyone can become a network node.
- ○ Anyone can enter records on the ledger.
- ◉ All of the above
- ○ Only the first two options are correct.

✓ **Correct**
On a public blockchain, anyone can view the ledger, become a network node, and enter records on the ledger.

4. Which of the following best describes a **permissioned** blockchain? **1 / 1 point**

- ○ A firm or consortium of firms controls who can view the ledger.
- ○ A firm or consortium of firms controls who can become a network node.
- ○ A firm or consortium of firms controls who can enter records on the ledger.
- ◉ All of the above
- ○ Only the second and third options are correct.

✓ **Correct**
With a permissioned blockchain, a firm or consortium of firms controls who can view the ledger, who can become a network node, and who can enter records on the ledger.

5. A private distributed ledger is: **1 / 1 point**

- ○ Permissionless
- ○ Trustless
- ○ Open
- ○ All of the above
- ◉ None of the above

✓ **Correct**
A private distributed ledger is permissioned, requires some degree of trust, and is not open to the public.

Whether public or private, in what sense does blockchain technology have a high level of **1 / 1 point**

6. transparency?

- (●) In principle, all transactions are traceable with attribution of assets to identifiers (e.g. addresses).
- ( ) In principle, anyone with access to the blockchain can decrypt any of its encrypted data.
- ( ) In principle, the real-world identities corresponding to each identifier (address) are known.
- ( ) In principle, only nodes with verified identities can join the network.

✓ **Correct**
On a public blockchain these identifiers (addresses) are pseudonymous. On a private blockchain, these identifiers may or may not be pseudonymous.

7. How can one party prove to another party that they know a value, *x*, without revealing *x*itself (or any additional information). **1 / 1 point**

- ( ) private key
- (●) zero-knowledge proof
- ( ) total-knowledge proof
- ( ) probabilistic proof

✓ **Correct**
A zero-knowledge proof enables one party prove to another party that they know a value, *x*, without revealing *x*itself (or any additional information).

8. Which of the following is an approach to privacy that conceals one's identity by algorithmically generating a new public/private key pair for every transaction, based on a single master seed key? **0 / 1 point**

- ( ) zk-SNARK
- ( ) consortium blockchain
- (●) classic exchange wallet
- ( ) hierarchical deterministic (HD) wallet

! **Incorrect**
Please refer to the video "Usage of Multiple IDs" in Module 3, Lesson 4 for more information.

9. How could blockchain technology assist in reducing the asymmetry of information between a firm and its shareholders? **1 / 1 point**

- ○ It can't; implementing blockchain technology would actually *increase* the asymmetry of information between a firm and its shareholders.
- ◉ By providing shareholders with a fully traceable record of the firm's business dealings (e.g. asset ownership, transactions, and contracts), provided that the firm's addresses are fully disclosed.
- ○ By allowing the firm to selectively disclose a subset of its information in order to build a good reputation.
- ○ By providing shareholders with intermittent accounting reports which have been certified by a trusted third party.

✓ **Correct**

Blockchain has a high native level of transparency, which can help reduce information asymmetries.

10. In which scenario would it make sense for an organization to adopt a **consortium**blockchain? **1 / 1 point**

- ○ A dictator wants to conceal the corruption in his government's land title registry.
- ○ A medical lab wants to have exclusive write-access for recording patient records.
- ◉ A financial institution wants to leverage the network effects and cryptographic auditing capabilities of a blockchain, however they are required by law to follow KYC/AML regulations.
- ○ All of the above

✓ **Correct**

The R3 Consortium is an example of this.