Hardware Encryption (1 of 3)

- Software encryption can be subject to attacks to exploit its vulnerabilities
- Cryptography can be embedded in hardware
  - Provides higher degree of security
  - Can be applied to USB devices and standard hard drives
- Hardware encryption options include:
  - Trusted platform module
  - Hardware security model

Hardware Encryption (2 of 3)

- **USB device encryption**
  - Encrypted hardware-based flash drives can be used
    - Will not connect a computer until correct password has been provided
    - All data copied to the drive is automatically encrypted
    - Tamper-resistant external cases
    - Administrators can remotely control and track activity on the devices
    - Stolen drives can be remotely disabled
- **Self-Encrypting Drives (SEDs)**
  - Self-encrypting hard disk drives protect all files stored on them
  - The drive and host device perform authentication process during initial power up
  - If authentication fails, the drive can be configured to deny access or even delete encryption keys so all data is permanently unreadable

Hardware Encryption (3 of 3)

- **Hardware Security Module (HSM)**
  - HSM is a removable external cryptographic device
  - It includes an onboard key generator and key storage facility
  - Performs accelerated symmetric and asymmetric encryption
  - Malware cannot compromise it
- **Trusted Platform Module (TPM)**
  - TPM is a chip on a computer's motherboard that provides cryptographic services
  - Includes a true random number generator
  - Entirely done in hardware so it cannot be subject to software attack
  - Prevents computer from booting if files or data have been altered
  - Prompts for password if hard drive moved to a new computer

Blockchain (1 of 3)

- A **blockchain** is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network
- Blockchain technology allows a network of computers to agree at regular intervals on the true state of a distributed ledger
- It is a system in which a record of transactions made is maintained across several computers that are linked in a peer-to-peer network
- Blockchain relies on cryptographic hash algorithms to records its transactions

Blockchain (2 of 3)

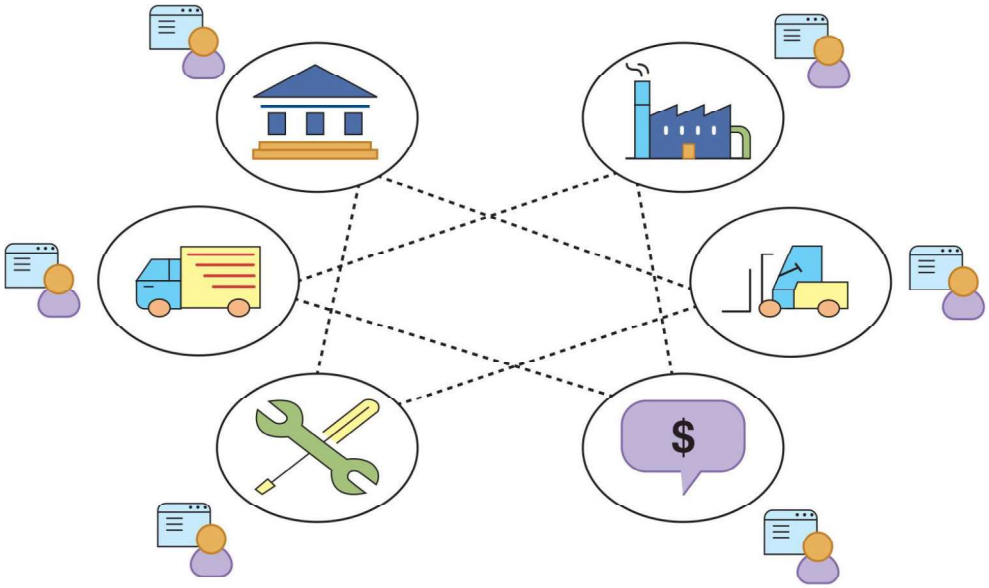

Figure 6-12 Multiple organizations with ledgers

Figure 6-12 Multiple organizations with ledgers

Blockchain (3 of 3)

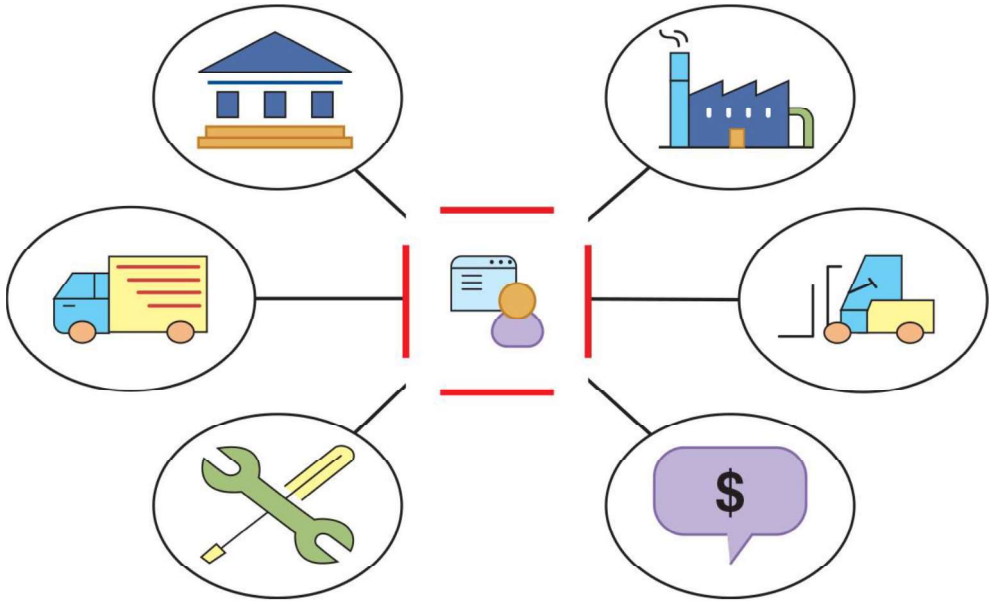

Figure 6-13 Multiple organizations using single ledger

Figure 6-13 Multiple organizations using single ledger

Knowledge Check Activity 4

Which of the following is an example of FDE?

a. BitLocker
b. EFS
c. GNuPG
d. Folder Lock

Knowledge Check Activity 4: Answer

Which of the following is an example of FDE?

Answer: a. BitLocker

BitLocker encrypts the entire system volume and prevents attackers from accessing data by booting from another OS. The other encryption methods encrypt individual files, folders, or transmitted data.

Self-Assessment

Complete Case Projects 6-2 and 6-3. After completing them, use your knowledge to consider these questions: What are the downsides to using encryption to secure your data on your own devices? How easy is it to encrypt your data and what are the possible consequences of not encrypting your data?

Summary (1 of 2)

- Cryptography is the practice of transforming information into a secure form so that unauthorized persons cannot access it
- Cryptography can provide confidentiality, integrity, authentication, nonrepudiation, and obfuscation
- One variation of a cryptographic algorithm is based on the device that is used in the cryptographic process
  - Another variation is the amount of data that is processed at a time
- Hashing creates a unique digital fingerprint called a digest, which represents the contents of the original material
- Symmetric cryptography (also called private key cryptography) uses a single key to encrypt and decrypt a message

Summary (2 of 2)

- Asymmetric cryptography (also known as public key cryptography) uses two keys instead of one
- Because cryptography provides a high degree of protection, it remains under attack
- Quantum computing relies on quantum physics using atomic-scale units (qubits) that can be both 0 and 1 at the same time
- Cryptography can be applied through either software or hardware
- Hardware encryption cannot be exploited like software cryptography
- A blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network