Lesson Plan: Blockchain and Bitcoin

Assignment

Listening assignment:

Listen to the “Blockchain and Bitcoin” episode of the “How Hacks Happen” podcast.

- Length: 50 minutes
- Where to listen: On most popular podcast platforms, search for “How Hacks Happen”. You may also listen at https://howhackshappen.net/episodes.

Reading assignment:

- "A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto, particularly sections 1, 2, 5, and 12.

Discussion Questions

Q. What are some common uses for hashing?

Q. Bitcoin and other cryptocurrencies are an entirely new way of controlling and exchanging money. Do you think this is type of currency is a fad, or will it last?

Q. What are some of the advantages of an anonymous currency? What are some of the disadvantages?

Q. Draw a diagram showing how the blockchain is constructed. (Hint: the paper by Satoshi Nakamoto has some diagrams that can help.)

Q. What does “mining” mean in relation to Bitcoin?

Q. How is it that blockchain imparts trust that all the transactions in the chain will be safeguarded?

Q. There are 18 million Bitcoin already in circulation, and it is estimated that it will take another 120 years before the cap of 21 million is reached. Do you think this estimate is accurate? What do you think will happen to the Bitcoin market when the 21 million mark is reached?

Q. What are some other cryptocurrencies that are in circulation? Which ones use blockchain?

Q. Why do you think Satoshi Nakamoto chose to keep his/her identity secret?

Q. Discuss the pros and cons of the various methods of keeping the cryptographic key that you’d need to access your Bitcoin (cold wallet, online exchange, etc.)

Lesson Plan: Blockchain and Bitcoin

Quiz/Assignment Questions

These questions can be posed as essay questions for quiz or assignment, or as multiple-choice questions. For multiple choice, the correct answer is indicated by a checkmark (✓) and some suggested wrong answers are indicated with (x).

Q. What is the difference between currency and stock?

- ✓ Currency can be used to purchase items, while stock can only be bought and sold.
- x Currency is a much more stable and secure investment than stocks.
- x Stocks are a much more stable and secure investment than currency.
- x Stocks can be purchased through a broker, but currency can't.

Q. What is the primary use of hashing as it's used in cybersecurity?

- ✓ For comparison of two files
- x To encrypt sensitive documents
- x To hide the contents of files from prying eyes
- x For submitting films to film competitions
- x To smash ceramic tiles with tiny robots

Q. Which of the following are true of the hashing process? (multiple answers)

- ✓ It's irreversible—you can't figure out the original contents from the hash.
- ✓ The hash of a large file is comparatively small.
- ✓ If you hash the same file over and over with the same algorithm, you get the same hash.
- x Hash algorithms are secret, which is what keeps them secure.
- x Two completely different inputs often produce the same hash.

Q. What was the reason the originator of blockchain and Bitcoin gave for his proposal?

- ✓ To provide a means for control and anonymity in financial transactions, without reliance on a third party.
- x To create a currency for anonymous purchases of illegal contraband and guns on the dark web.
- x To set up a more reliable investment method for investors, to help them gain wealth without the risk of investing in stocks.
- x To create a means to store and retrieve transactions more efficiently.

Lesson Plan: Blockchain and Bitcoin

Q. What is a blockchain puzzle?

- ✓ A challenge to add random characters to a block to produce a hash with certain characteristics.
- x A race to find the cryptographic key associated with the transaction, to unlock the contents of the block.
- x A race to be the first one to access the transaction when it goes out to the network.
- x A challenge to compare multiple chains to make sure they're the same.

Q. If blockchain transactions are anonymous, how can you identify and claim your cryptocurrency transactions?

- ✓ Each transaction is associated with a cryptographic key. If you have the key, you can access the transactions.
- x You can claim a transaction if you can solve the hashing puzzle associated with it.
- x A hash of your name and Social Security Number is included with each transaction associated with you.
- x Your bank's routing number, and your bank account number, are included with each transaction associated with you.

Q. How are new Bitcoins "minted" (brought into circulation)?

- ✓ Whenever a new block is added to the blockchain, the entity that solved the puzzle gets some new Bitcoin.
- x Satoshi Nakamoto periodically transfers a set quantity of Bitcoin to a digital vault for circulation.
- x The Bitcoin network holds the Bitcoin in a special blockchain and distributes it whenever a new transaction is originated.
- x All Bitcoins are already in circulation, and no new ones are being minted.

Q. If you lose the cryptographic key that pertains to your Bitcoin, how can you recover it?

- ✓ You can't recover a lost cryptographic key. It's gone forever.
- x You can contact the Bitcoin Repository and, for a small fee, they will send you a copy of the key.
- x You can make up a new key and use that to recover your transactions.
- x You can use face ID, fingerprint, or some other identification to recover the key.

Q. Who is Satoshi Nakamoto?

- ✓ Nobody knows for sure.
- x A pseudonym for a group of Japanese hackers.
- x A Japanese researcher specializing in cryptographic algorithms.
- x A pseudonym for an unknown manga artist.