Videos: Solutions

Bitcoin and Cryptocurrency Technologies

CHAPTER 1: INTRODUCTION TO CRYPTO AND CRYPTOCURRECIES

1. **Cryptographic hash functions**

   Which of the following is true of SHA-256?

   (a) It has been proven not to have a collision

   (b) We hope that there are no collations

   (c) No collision has ever been found

   (d) It has been proven that there is not fast way to find collisions

2. **Hash pointer and data structures**

   Which of the following types of modification of a block chain data structure can be detected?

   (a) Insertion of a block

   (b) Deletion of a block

   (c) Tampering of data in a block

   (d) Re-ordering of block

3. **Digital signatures**

   Which of these keys are required for verifying a signature?

   (a) The secret key

   (b) The public key

   (c) Both the secret key and the public key

   (d) Node. Keys are required only for signing; anyone can verify the signature without a key

4. **Public key as identities**

   If you generate numerous identities (public keys) for yourself and interact on line using those different identities, what might happen?

(a) Others might be able to take over your identities if your randomness is bad

(b) Others may be able to link you identities because public keys generated on the same computer look similar

(c) Others may be able to de-anonymize you by analyzing your activity patterns

5. **A simple Cryptocurrency**

In Scrooge Coin, you have ten coins each of value 3.0. You'd like to transfer coins of value 5.0 to your friends. This require.

(a) One transaction, one new coin created, and one signature

(b) One transaction, two new coins created. And two signatures

(c) Two transaction, two new coins created, and four signatures

(d) Two transaction, one new coins created, and two signature

CHAPTER 2: HOW BITCOIN ACHIEVES DECENTRALIZATION

1. **Centralization vs. Decentralization**

Which of these factors make distributes consensus hard?

(a) Nodes may crash

(b) Nodes maybe be taken over by malware

(c) Encrypted message may be intercepted and decrypted

(d) There is latency on the network

2. **Distributed consensus**

Why is bitcoin able to reach consensus in practice despite this being a generally difficult problem?

(a) Financial incentives cause participant work together

(b) Only small groups of nodes have to reach consensus rather than the network having to globally reach consensus

(c) The order of blocks doesn't matter for consensus

(d) Consensus only has to be reached over long time scales

3. **Consensus without identities: the block chain**

What can a malicious node do?

(a) Create valid transactions originating from someone else address

(b) Prevent a valid transaction from getting any confirmations

(c) Ignore the longest valid branch rule when proposing a new block

4. **Incentives of proof of work**

Proof of work is a way to:

(a) Select nodes in proportion of computing power

(b) Let nodes compete for the 'right' to creates blocks

(c) Make it impossible for one miner to act like many different miners

A block in the block chain was found at time t. what is the probability that next block was found at or before t + 10 minutes? Assume that the total hash power stay constant.

(a) More than 50%

(b) Less than 50%

(c) Exactly 50%

5. **Putting it all together**

A 51% attacker can potentially:

(a) Steal coin from an existing address

(b) Make it unprofitable for other miners to mine

(c) Change the block reward

(d) Suppress transactions form the block chain

Which of the following are true?

(a) 51% attacks are difficulty because an adversary would need to control more than half of the nodes on the bitcoin network

(b) Proof-of-work is essential for preventing Sybil attacks on the bitcoin blockchain

(c) As a transaction gets buried deeper in the blockchain, it becomes less and less likely that it will ever be undone because the work require to make a longer alternate branch becomes more and more difficult

CHAPTER 3: MECHANICS OF BITCOIN

1. **Bitcoin transactions**

In a typical transaction

(a) There is one signature that covers all the inputs

(b) Each input contains a signature

(c) There is one signature that covers all the output

(d) Each output contains a signature

2. **Bitcoins Scripts**

Bitcoin's script supports instructions whose effect is:

(a) Adding two numbers

(b) Conditions execution (if/then)

(c) Looping

(d) Recursion

(e) Hashing

3. **Applications of bitcoin scripts**

Alice is paying for a service using bitcoin micropayments. If she simply disconnects at some point without notifying Bob and stops sending micropayments. What can Bob do?

(a) Bob is out of luck. He doesn't earn any bitcoin and must pursue legal recourse

(b) Bob can redeem the maximum amount that Alice initially escrowed into a multisig address

(c) Bob can redeem the latest micropayment transaction that Alice sent in the last time period before disconnecting, which matches the length of services she received.

(d) Bob can refuse to sign the refund transaction, so both Alice and Bob will end up losing Bitcoins, which will sit in the multisig escrow forever

Bitcoin micropayments require the use of:

(a) Multisignature transactions

(b) Proof of burn

(c) Time-locked transactions

(d) Pay-to-script-hash

4. **Bitcoin blocks**

Blocks contain a tree of transactions instead of a flat list because:

(a) It result is smaller blocks

(b) It´s easier to insert or delete new transactions while the block is being assembles

(c) It enables efficiently proving that a transaction is include in a block

5. **The bitcoin network**

If two transactions A–>B and A<–C are both broadcasted almost simultaneously from different modes, what determines which one will eventually end up in the block chain?

(a) The transaction that reaches the majority of nodes first will win

(b) The transactions that was broadcast first will win

(c) The miner who finds the next block will likely resolve the tie by including one of the transactions in the block

(d) Each node has its own version of the block chain containing the transaction that it heard about first

6. **Limitations and improvements**

Which of the following requires a hard fork?

(a) Disabling the OP_SHA1 instruction

(b) A requirement that each transaction have it outputs sorted by values in ascending (or not-decreasing) order

(c) Increasing the maximum permitted size of blocks

(d) Decreasing the maximum permitted size of blocks

(e) Adding a new OP_SHA3 script instruction

CHAPTER 4: HOW TO STORE AND USE BITCOINS

1. **How to store and use bitcoins**

What is bitcoin wallet?

(a) An address that contains a lot of unspent bitcoins

(b) A piece of software that remember an individual's bitcoins address and keys

(c) A type of mining software

(d) An online exchange that people can go to in order to acquire bitcoins

2. **Hot and cold storage**

Which of the following statements are true about cold wallet storage? (check all that apply)

(a) Cold storage stores keys in a device without network access

(b) Cold storage tends to be more convenient

(c) Cold storage can store more bitcoins

(d) Hot storage wallets can generate arbitrarily many cold storage addresses without contacting the cold storage

3. **Splitting and sharing keys**

In the K-out-of-N secret sharing scheme presented, the size of each share (in bits) will be

(a) 1/K times the size of the secret

(b) Equal to the size of the secret

(c) K times the size of the secret

(d) N times the size of the secret

4. **Online wallets and exchanges**

   Which of these are risks of Bitcoin exchanges that are NOT risks of maintaining one's own hot or cold wallet? (check all that apply)

   (a) Bank runs

   (b) Ponzi schemes

   (c) Key compromises or leaks

   (d) Double-spend attacks

5. **Payment services**

   In the scenario presented, which of these parties are exposed to exchange rate risk? (check all that apply)

   (a) User

   (b) Merchant
   The user is exposed to exchange rate rick to some degree since they must hold bitcoins at least temporally to be able to pay whit bitcoins.

   (c) Payment service

6. **Transactions fees**

   Doesn't have questions

7. **Currency exchange markets**

   In the model presented, which of these are sources of demand for bitcoins? (check all that apply)

   (a) Mediating fiat-currency transactions
   The model presented considered only two sources of demand: meadiating fiat-currency transaction and investment. Theoretical model must often leave out some factors that matter in practice in order to keep the analysis tractable. Arguably, paying transaction fees is also a source of demand for bitcoins.

   (b) Demand deposits of bitcoins

   (c) Gambling

   (d) Investment
   The model presented considered only two sources of demand: meadiating fiat-currency transaction and investment. Theoretical model must often leave out some factors that matter in practice in order to keep the analysis tractable. Arguably, paying transaction fees is also a source of demand for bitcoins.

   (e) Paying transaction fees

CHAPTER 5: BITCOIN MINING

1. **The task of Bitcoin Miners**

   Which of the following are true about Bitcoin miners?

   (a) The target hash has become so small that the block header nonce alone isn't generally large enough to allow miners so search enough of the hash output space to find a valid block

   (b) Bitcoin miners can more efficiently mine for blocks by specifically targeting parts of the nonce search space that have more puzzle solutions

   (c) Over a 2 week period, the average time to mine a block is always 10 minutes

   (d) The mining difficulty is recomputed roughly every 2 weeks to keep the proof-of-work puzzle difficult

2. **Mining Hardware**

   Which statement about Bitcoin miners is NOT true?

   (a) If the global hash rate doubles every two months, a new piece of hardware that a miner buys will find most of the blocks that it ever will mine in the first six months of operation

   (b) Bitcoin miners can recoup a reasonable fraction of their initial expenses by selling their ASICs once they are done with them to other users for less computationally intense purposes

   (c) Many miners will consider the climate of an area when setting up mining operations because of the cost of cooling their equipment

   (d) Mining Bitcoin on a modern CPU will yield negligible mining rewards

3. **Energy Consumption & Ecology**

   Which of the following are assumptions made about the UPPER bound for the energy used for mining Bitcoins? (check all that apply)

   (a) Everyone mines where it is cold (cooling doesn't consume energy)

   (b) Everyone mines at the maximum claimed efficiency

   (c) Miners mine up to the point that all of the money they earn is used to pay for electricity

   (d) The energy efficiency of mining hardware decreases with age

   (e) Miners all pay the same for electricity

   Which of the following are assumptions made about the LOWER bound for the energy used for mining Bitcoins? (check all that apply)

   (a) Everyone mines where it is cold (cooling doesn't consume energy)

   (b) Everyone mines at the maximum claimed efficiency

   (c) Miners mine up to the point that all of the money they earn is used to pay for electricity

   (d) The energy efficiency of mining hardware decreases with age

4. **Mining Pools**

   Mining pools...

   (a) Let members earn more rewards, on average, than they would by mining alone

   (b) Typically make all their members search for blocks with the same coinbase address (the address that receives mining rewards)

   (c) Evenly divide up block rewards between all members of the pool

   (d) Can undermine the security of Bitcoins consensus algorithm, but this isn't a problem in practice since the majority of miners aren't part of pools

5. **Mining Incentives and Strategies**

   Which of the following are true about potential mining strategies Bitcoin miners can employ? (check all that apply)

   (a) Miners who control more mining power have more potentially profitable strategies available

   (b) Block withholding, forking, and other attacks have been frequently carried out in practice

   (c) Some alternative strategies might be motivated by goals other than earning more bitcoins

CHAPTER 6: BITCOIN AND ANONYMITY

1. **Anonymity Basics**

   Unlinkability in Bitcoin could mean

   (a) It's hard to link different address owned by the same user

   (b) It's hard to link different transactions made by the same user

   (c) It's hard to link different transactions having the same output address

2. **How to de-anomymize Bitcoin**

   Which of the following observations would suggest that address A and B may be controlled by the same user/entity

   (a) There is a transaction with A as a input address and B as output addresses

   (b) There is a transaction with both A and B as input addresses

   (c) There is a transaction with both A and B as output addresses

3. **Mixing**

   Which of these techniques can improve the anonymity provide by mixing services?(check all that apply)

(a) Using a series of mixes

(b) Using the same 'chunk' size for all mixing transactions

(c) Charging a constant percentage of the transaction value as a mixing fee

4. **Decentralized Mixing**

Which of these is NOT an advantage of CoinJoin over centralized mixes

(a) There by mixes is impossible

(b) Built-in protection against denial-of-service attacks

(c) Potentially better anonymity because centralized mines can e compromised by adversaries.

5. **Zerocoin and Zerocash**

What is 'zero knowledge' about zero-knowledge proof?

(a) It take no outside knowledge to verify the correctness of the proof

(b) It is proof that doesn't reveal any knowledge to create

(c) It is a proof that requires no knowledge to create

(d) It is a proof that you have no knowledge of something

6. **Tor and the Silk Road**

Doesn't have questions

CHAPTER 7: COMMUNITY, POLITICS, AND REGULATION

1. **Consensus in Bitcoin**

Doesn't have questions

2. **Bitcoin Core Software**

Which of the following is true about a fork of Bitcoin's rules which results in a fork of the block chain into two branches?

(a) Anyone who owned bitcoins before the fork can choose which branch to transfer their coins to

(b) The fork will eventually be resolved due to the longest valid branch rule

(c) The fork doubles the total value of the currency

(d) A transaction can be valid in both forks

3. **stakeholders: Who's in charge?**

   Which participants in the Bitcoin ecosystem have some amount of power in a negotiation about rule-setting?

   (a) Bitcoin Core developers

   (b) Miners

   (c) Investors

   (d) Merchants

   (e) Payment services

4. **Roots of Bitcoin**

   Doesn't have questions

5. **Governments Notice Bitcoin**

   According to the lecture, what's one way that governments have tried to enforce capital controls in a world with Bitcoin?

   (a) Shutting down Bitcoin-based markets for illegal items such as Silk Road

   (b) Disconnecting Bitcoin from the local fiat currency

   (c) Blocking the Bitcoin protocol

   (d) Purchasing mining hardware and attempting a Goldfinger attack

6. **Anti Money-Laundering**

   According to the lecture, what steps do governments take to prevent money laundering? (Check all that apply)

   (a) Require some businesses that handle money to know their customers identities

   (b) Constantly monitor the Bitcoin network and block chain

   (c) Require a variety of companies to file reports describing any large transactions they are a party to

   (d) Limit the maximum size of financial transactions

7. **Regulation**

   A reputation-based approach to fixing a lemons market might not work:

   (a) At the end of a seller's presence in the market

   (b) When sellers don't provide warranties for products

   (c) When consumers don't do repeat business with the same entity

   (d) At the beginning of a sellers presence in the market

Which of these are signs that there might be a market failure?

(a) The market is completely unregulated

(b) Sellers agree with each other to raise prices

(c) Sellers agree not to compete with each other and offer a reduced selection of products

8. **New York's BitLicense Proposal**

   Doesn't have questions

CHAPTER 8: ALTERNATIVE MINING PUZZLES

1. **Essential Puzzle Requirements**

   Doesn't have questions

2. **ASIC Resistant Puzzles**

   ASIC resistance...

   (a) seeks to make it more appealing to mine with regular consumer devices than it is today

   (b) has been successfully achieved in practice using the 'script' memory-hard hash function

   (c) is a response to the centralization of Bitcoin mining

3. **Proof-of-usefol-work**

   Proof-of-useful-work cryptocurrency designs...

   (a) differ from traditional volunteer distributed computing projects because cryptocurrencies cannot rely on a trusted administrator to select and distribute the problems to be solved

   (b) have been successfully used to solve computational problems such as protein folding

   (c) should preferably be based on problems whose solution benefits the public, rather than the solver, to avoid skewing the incentives of miners

4. **Nonoutsourceable Puzzle**

   In a vigilante attack against a mining pool, the attacker,

   (a) discards both shares and blocks that he finds

   (b) submits shares but discards blocks

   (c) discards shares while submitting blocks to a different mining pool

5. **Proof-of-Stake 'Virtual Mining'**

   Which of these is true of virtual mining?

(a) Virtual mining does away with most of the power requirements of proof-of-work systems

(b) A proof-of-stake system makes 51% attacks impossible

(c) Several variations of virtual mining have been proposed

CHAPTER 9: BITCOIN AS PLATFORM

1. **Bitcoin as an Append-Only Log**

   In which of these situations could secure timestamping be useful? Assume that there is no way to prove that you didn't timestamp multiple values

   (a) Proving that you don't know something at a specific time

   (b) Proving possession of a document at a specific time

   (c) Securely saving a document at a specific time

   (d) Proving that you can predict the winner of the 2016 US presidential election

2. **Bitcoin as Smart Property**

   The OpenAssets protocol works by

   (a) Enabling conversion between Bitcoin and a new type of coin

   (b) Forking Bitcoin to allow many different types of "colored" coins

   (c) Associating extra metadata with bitcoins

   (d) Exploiting non-fungibility of bitcoins to impose a blacklist

3. **Secure Multi-Party Lotteries in Bitcoin**

   Which of the following features does the Bitcoin secure multi-party lottery system presented depend on?

   (a) Hash commitments

   (b) Colored coins

   (c) Multisignatures

   (d) Time-locked transactions

   (e) Micropayments

4. **Bitcoin as Randomness Source**

   Which of these are advantages of using the Bitcoin blockchain to generate a cryptographic beacon?

   (a) The beacon outputs random bits at frequent intervals

   (b) Fresh random bits can be obtained at any desired future time

(c) Manipulating the beacon output requires 51

(d) The cost to an attacker to manipulate the beacon's output is quantifiable

(e) No central authority is needed

5. **Prediction Markets & Real-World Data Feeds**

In a prediction market where shares pay out if and only if a potential future event happens:

(a) The average price of all shares traded as a fraction of the payout is an estimate of the event's likelihood

(b) The current price of shares as a fraction of the payout is an estimate of the event's likelihood

(c) A trader who is able to control or influence the outcome of the event will likely be able to make a profit

CHAPTER 10: ALTCOINS AND THE CRYPTOCURRENCY ECOSYSTEM

1. **Short History of Altcoins**

Which of these statements about altcoins are true?

(a) Bitcoin has a higher "market capitalization" than all altcoins combined

(b) Bitcoin is the most widely forked cryptocurrency

(c) Namecoin supports additional functionality such as domain-name registration that is not found in Bitcoin

2. **Interaction Between Bitcoin and Altcoins**

In a merge-mined altcoin scenario:

(a) Bitcoin blocks include transactions from the altcoin

(b) Altcoin block headers include a hash pointer to a Bitcoin block

(c) Bitcoin block headers include the merkle root of transactions for an altcoin block

(d) The altcoin has the same hash target as Bitcoin at all times

3. **Lifecycle of an Altcoin**

Doesn't have questions

4. **Bitcoin-Backed Altcoins, 'Side Chains'**

Here are several ways in which new coins in an altcoin can be allocated to users. Which of these require changes to Bitcoin?

(a) All coins in the altcoin are generated through (merge) mining and are allocated to miners

(b) Altcoin allocation is ”grandfathered” from Bitcoin - every owner of bitcoins becomes the owner of a certain number of altcoins (in a fixed proportion of bitcoins to altcoins)

(c) Bitcoin is used as a ”reserve currency” for the altcoin - a unit of the altcoin can be created by putting 1 BTC into escrow; the bitcoin can be released by provably destroying one altcoin unit

(d) A unit of the altcoin is created by provably destroying one bitcoin

CHAPTER 11: THE FUTURE OF BITCOIN

1. **The Block Chain as a Vehicle for Decentralization**

   In the smart property scenario presented, where Alice sells her car to Bob via an atomic transaction:

   (a) Bob must make sure that Alice deletes her private key so that she does not retain the ability to activate the car

   (b) Alice and Bob must be physically near the car for the transfer of control to take effect

   (c) Requires modifications to Bitcoin because there is no way for two different people who don't trust each other to securely sign the same transaction

   (d) The protocol doesn't prove to Bob, before the sale, that the transaction output that Alice wants to sell him actually corresponds to the car he wants to buy

2. **Routes of Blockchain Integration**

   Which of these are potential ways to improve security when using Bitcoin as a platform for decentralized commerce?

   (a) Atomic exchange

   (b) Reputation

   (c) Warranties

   (d) Escrow and dispute mediation

3. **What Can We Decentralize?**

   Data feeds...

   (a) allow arbiters to assert facts about the world into the block chain

   (b) are useful for implementing decentralized prediction markets

   (c) can be decentralized to a degree using Multisignature

4. **When is Decentralization a Good Idea**

   According to the lecture, what are some issues with using cryptography to enforce contracts?

(a) It is problematic if the state does not recognize a block chain based notion of property because the state will always be the final arbiter

(b) The technology behind smart contracts is not powerful enough to express the logic needed for real-world contracts like derivatives

(c) Cryptographic security lacks the corrective controls of real-world security such as prosecution of criminals

(d) Losing a device containing your private keys could result in the inability to use your smart property