Cryptocurrencies 2025W

Exam 1

- **Format:** "Multiple-Choice" but only **one** answer is correct for any given question.
- **Grading:** No negative points!
- **Note:** This version of the exam is copied by hand, expect typos. Some questions are missing.

1. Consider the following statements regarding the CAP theorem, the FLM and FLP impossibility results, and SMR protocols:

   - (A) FLM states that no SMR protocol can satisfy both safety and liveness deterministically or probabilistically in a fully asynchronous environment if a single crash-fault exists.
   - (B) FLP states that no SMR protocol guarantees both safety and liveness in a synchronous network if more than $\frac{1}{3}$ of participants are Byzantine, even if PKI is available.
   - (C) Quorum-based SMR protocols (e.g., PBFT, Tendermint, HotStuff) lose both liveness and safety during network partitions and only restore them during synchronous periods.
   - (D) Longest-chain SMR protocols (e.g., Bitcoin) maintain liveness but may lose safety during network partitions.

   Which of the statements above is **correct**?

   a. (A), (B), (D),
   b. (A), (D),
   c. Only (D),
   d. None of the above

2. Consider the following statements regarding consensus, state machine replication, and reliable broadcast. Which of the statements is **incorrect**?

   a. We can use a reliable broadcast protocol together with a view-change mechanism to solve consensus.
   b. Any protocol that solves consensus also solves state machine replication.
   c. We can use a consensus protocol to solve reliable broadcast.
   d. Reliable broadcast does not guarantee that correct nodes output a value when the sender is malicious.

3. Which of the following statements is **incorrect** about consensus?

   a. A protocol that achieves consensus in the partially synchronous network also achieves consensus in the synchronous network.
   b. Partial synchrony assumes the existence of an unknown Global Stabilization Time (GST), after which message delays are bounded.
   c. In a partially synchronous network, it is possible to run an asynchronous consensus protocol before GST and switch to a synchronous consensus protocol after GST, since nodes can safely detect that GST has occurred.
   d. Although a consensus protocol in a partially synchronous network may be live before GST (i.e. validators may be able commit blocks), liveness is guaranteed only after GST.

4. Consider an SMR protocol run by a network of nodes, where some nodes may be faulty. Which of the following statements is **correct**?

    a. If the faults are only crash faults, a node may send conflicting messages to different nodes before crashing.
    b. If the faults are only omission faults, a node may fail to send or receive messages but never sends incorrect or conflicting messages.
    c. If the faults are only Byzantine, a node may fail by stopping execution but will never send incorrect or conflicting messages.
    d. If the protocol tolerates Byzantine faults and guarantees both safety and liveness, it may fail to guarantee liveness if the Byzantine nodes are replaced with omission faults.

5. Consider a Dolev-Strong protocol execution with n nodes, out of which f are Byzantine. Which one of the following statements is **correct**?

    a. If we have an honest sender, all honest parties will have $n - f$ distinct signatures at round 1.
    b. If $f > \frac{n}{3}$, the Dolev-Strong protocol might not terminate.
    c. During round r, a node only accepts a value v if it is signed by $r - 1$ distinct other nodes.
    d. The protocol assumes that an adversary cannot forge signatures.

6. Which of the following is **correct** about PBFT, Tendermint, and HotStoff?

    a. Tendermint improves over PBFT in terms of view-change communication complexity, at the cost of giving away responsiveness.
    b. HotStuff improves over Tendermint in terms of responsiveness, at the cost of adding one extra voting phase.
    c. HotStuff improves over PBFT in terms of view-change communication complexity, at the cost of adding one extra voting phase.
    d. All the above.

7. [...missing...]

8. A system of $n = 3f + 1$ nodes, where exactly f nodes are Byzantine, runs a protocol Π to solve SMR in partial synchrony. The protocol Π is a variation of PBFT, differing in that each voting phase completes when nodes obtain a certificate containing exactly $q \neq 2f + 1$ votes. Which of the following statements is **correct**?

    a. For $q = 2f + 2$, the protocol Π satisfies safety, but not liveness.
    b. For $q = 2f + 2$, the protocol Π satisfies both safety and liveness.
    c. For $q = 2f$, the protocol Π satisfies safety, but not liveness.
    d. For $q = 2f + 2$, the protocol Π satisfies neither safety nor liveness.

9. A set of $n = 3f + 1$ nodes, out of which f are Byzantine, run the following protocol to achieve reliable broadcast. The network is asynchronous and we only assume authenticated channels. Specifically, we say that a protocol achieves reliable broadcast in asynchrony when the following properties hold:

   - **Validity:** If the leader is non-faulty, then eventually all non-faulty parties will output the leader's input.
   - **Totality:** If some non-faulty party outputs a value, then eventually all non-faulty parties will output a value.
   - **Agreement**: All non-faulty parties that output a value, output the same value.

   Designated leader: There is a node L which we call the leader. The leader broadcasts a value v to all nodes.

   Every node:
   (a) **Echo 1:** Upon receiving value v from the leader L, broadcast $< \text{echo} - 1, v >$ to all parties
   (b) **Echo 2:** Upon receiving $< \text{echo} - 1, v >$ from $n - f$ distinct nodes, broadcast $< \text{echo} - 2, v >$ to all parties.
   (c) **Decision:** Upon receiving $< \text{echo} - 2, v >$ from $f + 1$ distinct nodes, output v.

   Which of the following statements is **correct**?

   a. The protocol achieves realiable broadcast.
   b. The protocol satisfies validity and totality but not agreement.
   c. The protocol satisfies validity and agreement but not totality.
   d. The protocol satisfies agreement and totality but not validity.

10. A system of n always-online nodes, where f are Byzantine, runs the following protocol to agree on a sequence of values in the synchronous model.

    Leader Election: The execution is divided into views. In each view, a node is selected as the leader. Leaders are selected in a round-robin fashion.

    During a view: In each view, nodes run the Dolev-Strong protocol as the subroutine with the current leader as the designated sender.

    a. The protocol solves consensus in the unauthenticated setting (no PKI).
    b. The protocol realizes SMR for any $f < 2\frac{n}{3}$, even though clients do not monitor the execution of the protocol.
    c. There exists $f < n$ such that the protocol solves consensus, but does not realize SMR even if clients monitor the execution.
    d. None of the above.

11. Which of the following functions from $[0, \text{inf})$ to $[0, \text{inf})$ are collision-free?

    a. $H_1(x) = |x - 3|$
    b. $H_2(x) = (x - 2)^2$
    c. $H_3(x) = 2 + \cos(\pi x)$
    d. $H_4(x) = \frac{1}{2+x^5}$

12. Suppose an upgrade to Bitcoin adds a new script opcode that enables transaction inputs to be spent if the transaction has a certain number of outputs. This upgrade would be a:

    a. hard fork, which means nodes that do not upgrade will not accept such new blocks.
    b. hard fork, which means nodes that do not upgrade might mine invalid blocks.
    c. soft fork, which means nodes that do not upgrade will not accept such new blocks.
    d. soft fork, which means nodes that do not upgrade might mine invalid blocks.

13. Consider the *sorted* Merkle tree given in Figure 1. What would be a valid proof of non-inclusion of the value 5, assuming the root H_7 is known to everyone?

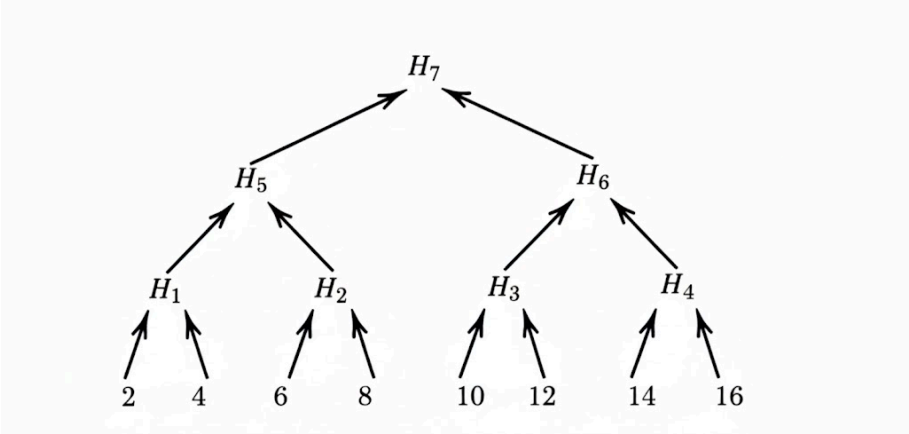


Figure 1: A sorted Merkle tree with leafs $\{2, 4, ..., 16\}$ and root H_7. The value H is the hash of the two values below. For example, $H_5 = H(H_1 \parallel H_2)$, with H a hash function.

    a. $(4, 6, H_1, H_6)$
    b. $(2, 4, 6, 8, H_6)$
    c. $(2, 4, H_2, H_6)$
    d. ~~$(4, 6, H_1, H_6)$~~

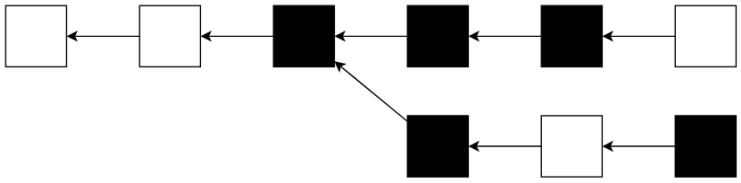
14. [...missing...]

15. In proving Bitcoin's security, why do we need to assume that no node has knowledge of the genesis block prior to the deployment of the protocol?

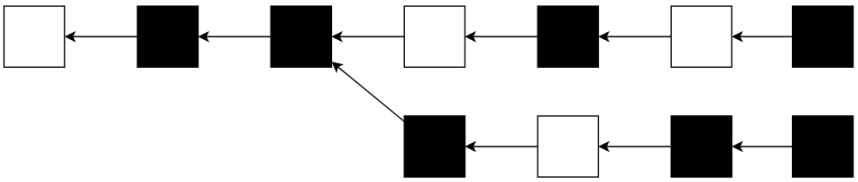
    a. Otherwise, the assumption that all nodes instantly learn about new block would not hold.
    b. The adversary could force different protocol rules by defining these in the first block.
    c. To make sure no adversary could have precomputed blocks.
    d. All of the above.

16. Assuming zero network delay ($\Delta = 0$) in the Bitcoin network, which of the following *cannot* occur?

(A)



(B)



(C)

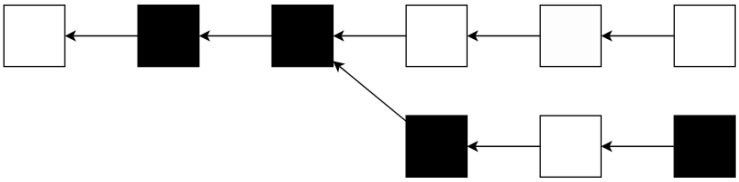


Figure 2: The figures depict blockchain forks. A white block is produced by an honest leader, whereas a black block is produced by a Byzantine leader.

a. (A),
b. (B),
c. (C),
d. (A) and (C).

17. [...missing...]

18. [...missing...]

19. Proof-of-Stake (PoS) vs Proof-of-Work (PoW): Which one of the following is **correct**?

a. It is computationally cheap to create valid blocks in a secure PoS consensus protocol like Ouroboros, unlike PoW consensus protocols like Bitcoin.
b. In Nakamoto consensus, miners do not need any key pair (unauthenticated setting), unlike PoS protocols like Ouroboros that require a PKI.
c. Long-range attacks are a fundamental security concern in PoS protocols due to weak subjectivity, whereas PoW protocols maintain security purely through cumulative computational effort.
d. All the above.

20. In a proof-of-stake longest chain protocol that uses VRFs for the leader election, like Ouroboros Praos, who can correctly predict which node will win the next block?

a. Anybody who knows the public keys of the nodes.
b. The adversary
c. Only the party that will win the next block.
d. Nobody.

21. Consider a (β_1, β_2)-secure Ebb-and-Flow protocol which uses PBFT $\left(\beta_1 = \frac{1}{3}\right)$ and Ouroboros Praos $\left(\beta_2 = \frac{1}{2}\right)$ as subprotocols. Which of the following is **correct**?

    a. The *final ledger* output by the Ebb-and-Flow protocol is *safe and live at all times*, assuming that the adversary controls less than β_1 of all nodes in the protocol.
    b. If $\mathrm{GST} = 0$, the *available ledger* output by the Ebb-and-Flow protocol is *safe and live at all times*, assuming that at any point in time, the adversary controls less than β_2 of the awake nodes in the protocol.
    c. The *available ledger* output by the Ebb-and-Flow protocol is *safe and live at all times*, assuming that the adversary controls less than β_2 of all nodes in the protocol.
    d. The Ebb-and-Flow protocol outputs two ledgers, with the available ledger being a prefix of the final one.

22. A blockchain of $n = 3f + 1$ replicas orders transactions correctly (safety + liveness), but replicas do *not* check transaction validity. Each replica locally executes the ordered ledger and signs a commitment to the resulting state at each block height.

    Assume at most f replicas are Byzantine and execution is deterministic.

    Which statement is **correct**?

    a. A client can trust a state commitment if it has signatures from at least $f + 1$ replicas.
    b. A client needs signatures from at least $2f + 1$ replicas to trust a state commitment.
    c. A client can accept a transaction if it is included in the ledger and is syntactically well-formed.
    d. Two honest replicas may sign different state commitments for the same height.

23. Let $\mathrm{sn}, \mathrm{pk}_i, \mathrm{sk}_i$, and T be the sequence number, the public key of user i, the secret key of user i, and the target. Consider a Proof-of-Stake longest chain protocol where the block proposer is elected according to inequality $H(\mathrm{sn}, \mathrm{pk}_i, \mathrm{prev\_hash}) < T$, where sn starts from value 1 and it is incremented by one only if no public key is elected as block proposer.

    Which of the following statements is **correct** about this protocol?

    a. It is unpredictable.
    b. It suffers from grinding attacks.
    c. It may never be live.
    d. It is not publicly verifiable.

24. Which of the following is **correct** about the weak subjectivity problem of PoS protocols?

    a. Weak subjectivity states that when a new node joins the network, if presented with multiple chains of the same length, it cannot identify the correct chain better than random guessing.
    b. Weak subjectivity is solved in the quasi-permissionless setting by assuming that honest parties delete their past keys.
    c. Weak subjectivity does not pose a problem for nodes that are always online and continuously monitor the protocol execution from the beginning.
    d. All the above.

25. Which of the following is **correct**?

    a. RanDAO used by Ethereum 2.0 is an unbiasable and unpredictable source of randomness.
    b. Ouroboros Praos has a public leader election mechanism based on Verifiable Delay Functions (VDFs).
    c. Snap-and-Chat protocols output two ledgers: one that is safe under network partitions and one that is live under dynamic participation.
    d. All the above.

26. Which of the following is **correct** about Algorand?

    a. Algorand is a longest chain protocol with adversarial resilience of $\frac{1}{2}$.
    b. Algorand has the highest notion of security because it remains secure assuming an asynchronous network.
    c. In the agreement phase, Algorand performs two voting rounds, selecting an independent, randomly sampled committee for each round.
    d. Algorand is not secure against a fully adaptive adversary.

27. Consider a simplified version of Ethereum 2.0 with a *static* validator set (i.e., no validators enter or exit during the protocol run). Assume the total stake 90 billion USD. Which statement is **correct** regarding Casper FFG security guarantees?

    a. If malicious validators control less than 45 billion USD of the total stake, then two conflicting checkpoints can never both be finalized.
    b. If malicious validators control more than 30 billion USD of the total stake, then conflicting checkpoints can be finalized and there is no way to punish the malicious validators.
    c. If malicious validators control more than 30 billion USD of the total stake, then in the event that two conflicting checkpoints are finalized, at least 30 billion USD of stake will be slashed.
    d. None of the above.

28. [...missing...]

29. Assume an attacker would be able to mount a 51% attack over 10 blocks, fully undetected. We assume the block reward is currently 50 BTC, and that the attacker holds 2 times the honest hashrate. What would be the cost of this 51% attack?

    a. 1000 BTC.
    b. 500 BTC.
    c. 0 BTC.
    d. This question cannot be answered as assumptions on miner commitment and price robustness are missing.

30. Contrary to Bitcoin, one can mine Monero only with CPUs or GPUs. Bitcoin's price and hashrate curently be around 65,000 EUR and $1.1 * 10^{21}$ hashes per second, respectively, whereas Monero's price and hashrate lie around 436 EUR and $6.5 * 10^{9}$ hashes per second. One may argue that Bitcoin is more costly to attack because:

    - (A) Most of Bitcoin mining is done with ASICs.
    - (B) Bitcoin's price is higher than Monero's price.
    - (C) Bitcoin's hashrate is higher than Monero's hashrate.

    Which of these statements is correct?

    a. (A) and (B),
    b. (A) and (C),
    c. (B) and (C),
    d. (A), (B), and (C).

31. Bitcoin's fee mechanism is a first-price auction, awarding block space to the highest bidder, at that highest bid. What is a drawback of this mechanism?

    a. Miners do not have a guaranteed minimum income.
    b. Miners can costlessly drive up the price users pay.
    c. It is hard for users to estimate an appropriate fee.
    d. Transaction fees can be altered afterwards.

32. Consider a fee mechanism that has no base fee but only a tip, where half of the tip is burned and the other half goes to the miner. Which of the following statements is **incorrect**?

    a. This fee mechanism will lead to an off-chain tip market.
    b. This fee mechanism is just a first-price auction.
    c. The burned portion of the tip allows users to set their own fees without considering what other users pay.
    d. During a spike in demand, high-value transactions can still be identified and accommodated.

33. Alice knows the privacy issue of Bitcoin from the Cryptocurrencies course 2025W, and plans to design a *Private-Bitcoin* with the following changes compared with the original Bitcoin protocol. Which of the following changes can solve the privacy problem while guaranteeing security at the same time?

    a. When the sender creates a transaction, the transferred amount is encrypted under the receiver's public key.
    b. Instead of broadcasting the transaction to the network, the sender transmits it privately to the receiver. The receiver reveals the transaction output only when later spending it.
    c. Inspired by ring signatures: the sender includes multiple input UTXOs of the same value that she controls, but does not reveal which one is actually spent to create the output.
    d. None of the above.

34. To address users' concerns about a centralized mixing service, Dave proposes a *decentalized* coin mixing protocol with Alice, Bob and Carol. Assume a synchronous network. The protocol is:

    (1) The four parties jointly agree on a single mixing transaction, including its set of inputs and outputs.
    (2) After verifying that the transaction is correct, each party produces a signature and shares it with the others.
    (3) The mixing succeeds once the fully signed transaction (containing all four signatures) is broadcast and confirmed on the Bitcoin blockchain.

    Which of the following statements about this protocol is **correct**?

    a. Since the network is synchronous, no party can cause the protocol to abort.
    b. In this protocol, a party who refuses to provide a valid signature can be identified.
    c. This protocol offers stronger unlinkability than the centralized scheme for all parties, including against Dave.
    d. None of the above.

35. A Zerocoin at its core is a commitment C for two values: (1) a serial number S; (2) random number r. Alice feels that it is difficult to remember the random number all the time, so she suggests making some changes to r instead of randomly selecting it. Which of the following new Zerocoin protocols is secure and also realizes privacy?

    a. Set $s = S$
    b. Set $r = c$, where c is a public constant value different from S.
    c. Assume there exists a public secure hash function H, whose input and output length are $|S|$ and $|r|$ respectively, and set $r = H(S)$.
    d. None of the above.

36. Assuming the blockchain miners are rational, how can they affect the Lightning Payment Channel protocol execution?

    a. They can stop signing the channel update request.
    b. They can steal the locked coins during channel opening.
    c. They can censor (i.e., not include) a commitment transaction that attempts to close the payment channel.
    d. They can leak one party's secret key to the counterparty.

37. Assume Bitcoin produces 6 blocks every hour. Which of the following statements [… missing …]

38. Consider 5 parties, Alice (A), Bob (B), Carol (C), Dave (D), and Eve (E), connected with each other through 4 payment channels: l_1, l_2, l_3 and l_4, as shown in Figure 3. Alice pays Eve 10 coins by using Hashed TimeLock Contracts (HTLCs), all relying on the same preimage. Each intermediary charges a fee of 1 coin. Bob and Dave collude to perform a Wormhole attack, bypassing Carol. How many coins do Bob and Dave have in total at the end of a successful attack?

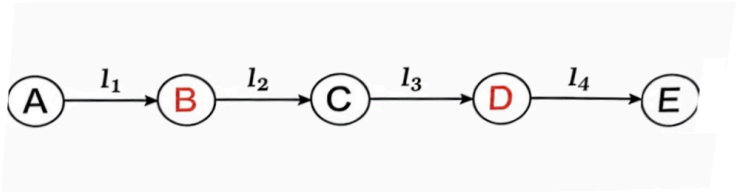


Figure 3: Topology of the channels.

a. 1.
b. 3.
c. 2.
d. 7.