Blockchain Foundations **NTUA, Spring, 2026**

Theory Exercise 2

Due: 14:00, Friday, Apr 10, 2026

Please solve all the problems below. The problems are worth equal points. After a genuine attempt to solve the homework problems by yourself, you are free to collaborate with your fellow students to find solutions to the theory homework problems. Regardless of whether you collaborate with other students, you are required to type up or write your own solutions. Copying homework solutions from another student or from existing solutions is a serious violation of the honor code. Please take advantage of the instructors' and TA's office hours. We are here to help you learn, and it never hurts to ask! The assignments should be written in LaTeX and submitted as a PDF file via Gradescope.

Problem 1

Consider the blocktree of Figure 1. Blue blocks are honestly mined blocks, whereas red blocks are adversarially mined blocks. Hypothetical blockids are shown within the squares.

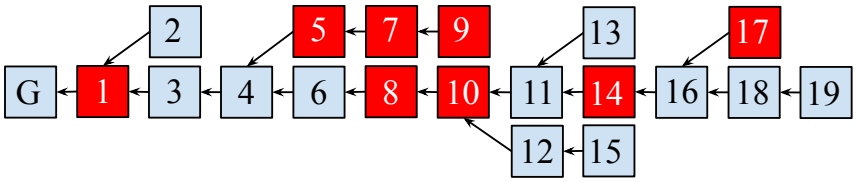

Figure 1: The blocktree.

Let $\mathcal{C}_1, \mathcal{C}_2$ indicate the chains whose tips are blocks 9 and 19 respectively.

1. What is the chain quality of $\mathcal{C}_1[-4:]$, $\mathcal{C}_1[:4]$ and $\mathcal{C}_2$ respectively?
2. Suppose an honest party had adopted $\mathcal{C}_1$ at time 100 and $\mathcal{C}_2$ at time 200. What is the velocity τ of the chain between those two times?

Problem 2

Consider $\Delta = 1, n = 5, t = 2$. Draw a timeline of successful queries that could have caused Figure 1 to appear. For each successful query, indicate:

1. The time at which it took place.
2. Whether the query was honest or adversarial.
3. The time at which each honest party received the block produced by the query.

For the timeline you drew, what is the *minimum* $k \in \mathbb{N}$ for which Common Prefix holds between *all* honest parties and across *all* time?

Problem 3

Consider the UTXO transaction graph illustrated in Figure 2. Hypothetical txids are shown within the circles. The value of an output is indicated above its respective arrow.

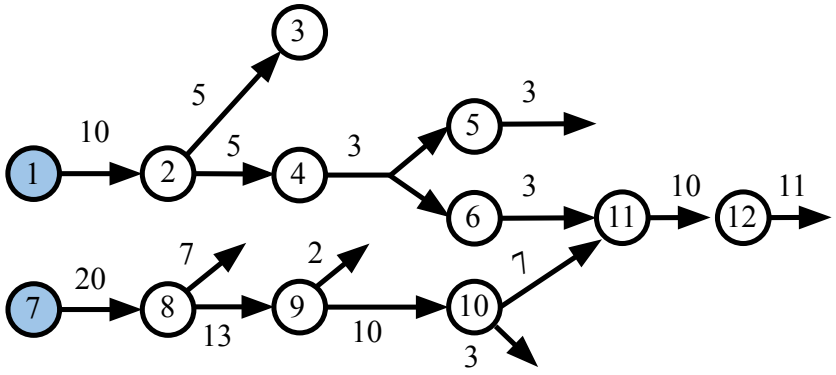

Figure 2: The transaction graph for Problem 3.

1. Honest party P has adopted a chain containing genesis (which has no transactions) and blocks B_1 (containing transaction 1 only) and B_2 (containing transaction 7 only) and is receiving the transactions from the network in this order: 2, 8, 9, 3, 4, 6, 5, 10, 11, 12. No other blocks beyond those three are mined. Which transactions will the mempool of this party contain?

2. The honest party managed to find a block B containing no new coinbase transactions and included its mempool on top of B_2. The rest of the honest parties then mine another k sequential blocks on top of B. No other blocks are mined in the meantime. What is the ledger L^P reported by the honest party P at the end of this process?

3. How much monetary value remains unspent in the system in the view of party P?

Problem 4

Consider the timeline of successful queries of Figure 3. The network delay is $\Delta = 1$, and we have $n = 3$ and $t = 0$.

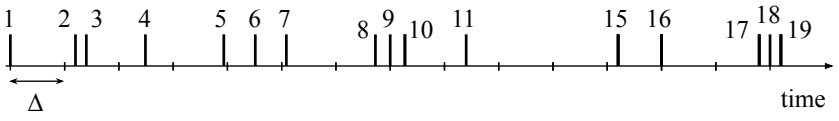

Figure 3: The timeline for Problem 4.

1. Indicate which among these successful queries are convergence opportunities.

2. Draw a blocktree that could have resulted from this timeline. For each block in the chain, indicate the successful query during which it was produced.

3. What is the height of the tip of the longest chain? What is the chain quality of the longest chain?

Problem 5

I was using the AI program ChatGPT to save some time while preparing the lecture notes for this course. As I was working on them, ChatGPT autocompleted my notes with the following text:

> It seems that all three properties, collision resistance, preimage resistance, and second preimage resistance, are desirable. However, it is not possible to have all three at the same time. In fact, the following theorem shows that it is impossible to have collision resistance and second preimage resistance at the same time.
>
> **Theorem 0.1** (Krawczyk's Theorem)**.** *Let $H : \{0,1\}^* \longrightarrow \{0,1\}^\kappa$ be a hash function. Then, H is collision resistant if and only if it is not second preimage resistant.*

Prove or disprove the above theorem. You may use ChatGPT and all the theorems we have proven in class. Good luck!

Reference

Some helpful definitions are provided below. For the full definitions, consult the lecture notes.

Definition (Collision Resistance)**.** A hash function $H : \{0,1\}^* \longrightarrow \{0,1\}^\kappa$ is *collision resistant* if for all PPT adversaries $\mathcal{A}$,

$$\Pr[\mathsf{collision\text{-}game}_{H,\mathcal{A}(\kappa)} = 1] = \mathrm{negl}(\kappa)\,.$$

The game is defined in Algorithm 1.

Algorithm 1 The collision-finding game for a hash function H.

```
function COLLISION-GAME_{H,A}(κ)
    x_1, x_2 ← A(1^κ)
    return H_κ(x_1) = H_κ(x_2) ∧ x_1 ≠ x_2
end function
```

Definition (2nd Preimage Resistance)**.** A hash function $H : \{0,1\}^* \longrightarrow \{0,1\}^\kappa$ is *2nd preimage resistant* if for all PPT adversaries $\mathcal{A}$,

$$\Pr[\mathsf{2nd\text{-}preimage\text{-}game}_{H,\mathcal{A}(\kappa)} = 1] = \mathrm{negl}(\kappa)\,.$$

The game is defined in Algorithm 2.

Algorithm 2 The second-preimage-finding game for a hash function H.

function $2\text{ND-PREIMAGE-GAME}_{\mathcal{A},H}(\kappa)$:
    $x_1 \xleftarrow{\$} \{0,1\}^{2\kappa}$
    $x_2 \leftarrow \mathcal{A}(x_1)$
    return $x_1 \neq x_2 \wedge H_\kappa(x_1) = H_\kappa(x_2)$
end function

Definition (Weak Conservation Law)**.** A transaction tx satisfies the Weak Conservation Law if

$$\sum_{i \in \mathsf{tx.ins}} i.v \geq \sum_{o \in \mathsf{tx.outs}} o.v\,.$$

Definition (Velocity)**.** The *velocity* τ of a chain of an honest party P between times $r_1 < r_2$ is the ratio $\frac{|\mathcal{C}^P_{r_2}| - |\mathcal{C}^P_{r_1}|}{r_2 - r_1}$.

Definition (Common Prefix)**.** A system is said to satisfy *Common Prefix* with parameter $k \in \mathbb{N}$ if for all honest parties P_1, P_2 and for all times $r_1 \leq r_2$, the chains adopted by the honest parties satisfy the property that

$$\mathcal{C}^{P_1}_{r_1}[:-k] \preceq \mathcal{C}^{P_2}_{r_2}\,.$$

Definition (Chain Quality)**.** A system is said to satisfy *Chain Quality* with parameters $\ell \in \mathbb{N}, \mu \in [0,1]$ if for all honest parties P and all times r, for all $i, j \in \mathbb{N}$ such that $j - i \geq \ell$, we have

$$\frac{|\mathcal{H}(C^P_r[i{:}j])|}{j - i} \geq \mu\,.$$

Definition (Chain Growth)**.** A system is said to satisfy *Chain Growth* with parameters $s \in \mathbb{N}, \tau \in \mathbb{R}^+$ if for all honest parties P and all times $r_1 \leq r_2$ such that $r_2 - r_1 \geq s$, we have

$$|C^P_{r_2}| - |C^P_{r_1}| \geq \tau(r_2 - r_1)\,.$$

Our variables.

- κ: The security parameter
- $\mathcal{A}$: The uniform PPT adversary
- Π: The honest protocol
- H: The hash function
- $\mathcal{G}$: The genesis block, an *honestly* mined reference block with 0 height
- Δ: The maximum network delay
- T: The mining target

- p: The probability of a successful query
- n: The total number of parties (includes both honest and adversarial)
- t: The number of adversarial parties
- q: The hashing power of a single party per unit of time
- k: The Common Prefix parameter, in blocks
- μ: The Chain Quality parameter, as a proportion
- τ: The velocity, in blocks per unit of time
- m: Epoch duration, in blocks

Chain addressing notation.

- $|\mathcal{C}|$: Chain length
- $\mathcal{C}[i]$: i^{th} block in the chain (0-based). The block height is i.
- $\mathcal{C}[-i]$: i^{th} block from the end.
- $\mathcal{C}[0]$: Genesis (by convention honest).
- $\mathcal{C}[-1]$: The tip.
- $\mathcal{C}[i{:}j]$: Chain chunk from block i (inclusive) to j (exclusive).
- $\mathcal{C}[{:}j]$: Chain chunk from the beginning and up to block j (exclusive).
- $\mathcal{C}[i{:}]$: Chain chunk from block i (inclusive) onwards.
- $\mathcal{C}[{:}-k]$: The stable chain.