Fundamentos y Aplicaciones de Blockchains

Homework 4

Depto. de Computación, UBA, 2do. Cuatrimestre 2025 *1/11/25*

Student: *Due: 13/11/25, 17:00 hs*

Instructions

- Upload your solution to Campus; make sure it's only one file, and clearly write your name on the first page. Name the file '<your last name>_HW4.pdf.'

  If you are proficient with LaTeX, you may also typeset your submission and submit in PDF format. To do so, uncomment the "%\begin{solution}" and "%\end{solution}" lines and write your solution between those two command lines.

- Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct.

- You may collaborate with others on this problem set. However, you must **write up your own solutions** and **list your collaborators and any external sources (including ChatGPT and similar generative AI chatbots)** for each problem. Be ready to explain your solutions orally to a member of the course staff if asked.

This homework contains 4 questions, for a total of 40 points.

1. **Bitcoin backbone: Chains of variable difficulty.**

   (a) (5 points) Describe Bahack's "difficulty raising" attack.

   Solution: El ataque consiste en tomar la cadena y agregar bloques con baja dificultad de minado (esta cadena no va a ser aceptada por los demás nodos, dado que será muy liviana) y crear todos los nodos de un epoch para esa cadena. Luego, aumetar mucho la dificultad (T) y, en caso de poder reslver la PoW rápido, tener de repente una cadena más pesada que las demás, conteniendo todos los bloques de baja dificultad previamente calculados

   (b) (5 points) What aspect of Bitcoin's target recalculation function makes the attack ineffective? Elaborate.

   Solution: El bitcoin target recalculation. Se pone un límite al ritmo en el que puede variar el nivel de dificultadde la prof of work (por ejemplo, 1/4T o 4T), de este modo, se previene el difficulty raising attack, y es seguro siempre y cuando el número de mineros no varíe de forma abrupta y constante. Esta asunción es razonable dado que el poder de cómputo es difícil de acumular.

2. **Proofs of Stake (PoS).**

   (a) (5 points) Consider the *long range attack* on a PoS blockchain in a permissionless environment. Assume that an honest-stake majority always holds, and that all the parties are aware of the global clock. Describe the scenarios wherein the honest parties lose their advantages, and explain why freshly joining parties cannot distinguish an honest chain from other chains by the longest-chain selection rule.

   Solution: Los miembros nuevos de la red no pueden distinguir entre la cadena honesta y la cadena del atacante ya que ambas parecen ser válidas desde su punto de vista.

   Se llama "Weak Subjetivity" al problema que tienen los nodos nuevos o que se reconectan luego de mucho tiempo para distinguir cadenas reales de cadenas alternativas. Esto ocurre ya que al momento de conectarse solo conocen el genesis node y tienen a la vista todas las cadenas publicadas, pero no tienen forma de distinguir cual es la main chain.

   En cambio, los nodos honestos que ya están corriendo aceptaron la cadena principal, y no van a aceptar otra a menos que esa otra se vuelva la principal.

   Fuente

   (b) (5 points) A PoS protocol performs leader election based on the stakes each party owns. Recall that the initial stake distribution is hard-coded in the genesis block. Does a PoS protocol assume a PKI? Further, the stakes in a party's account have monetary values. Where can the initial stakes come from?

   Solution: Si bien es necesario un método confiable para distribuir las claves privadas de las cuentas pertenecientes al genesis block y distribuirlas entre los participantes iniciales, la forma de hacerlo queda a decisión de cada blockchain. No se asume PKI, sin embargo, podría utilizarse un medio centralizado para hacer la distribución de los stakes iniciales, lo que necesitaría algún tipo de PKI.

3. **Verifiable Random Functions (VRFs).**

(a) (4 points) Enumerate the security properties a VRF should satisfy.

Solution: Una VRF debería satisfacer la propiedad principal: Dado un par (VK,SK) y un input X produce una variable pseudoaleatoria única verificable.

Para poder realizar esto cada usuario necesita un par que contiene una clave de verificación y una clave secreta. Luego, al momento de querer utilizarlo para un valor x dado, se genera el valor aleatorio y una prueba. Esto permite que la función sea (pseudo)aleatoria, dado que el valor generado es impredecible.

Más tarde, otro usuario puede utilizar la clave pública, el valor de X, el valor aleatorio generado y la prueba para llevar a cabo la verificación. Esto permite que la función sea verificable.

Además, para cada valor de X, el valor generado será único.

(b) (6 points) We stated in class that given a hash function, modeled as a *random oracle*, and an unforgeable signature scheme, VRFs are readily realizable. Show that that's indeed the case by proposing a construction and arguing its security—i.e., it achieves the desired security properties. Follow the VRF terminology we used in class.

Solution: Utilizamos la clave pública y clave privada del esquema de firmas digitales como las VK y SK de nuestra VRF. Keygen entonces es igual a la keygen de nuetro esquema.

$$VRF\_keygen(r) = DS\_keygen(r)$$

Para implementar Eval vamos a hacer una firma de X y luego aplicarle un hash a la firma, obteniendo un valor aleatorio (podemos afirmar que es aleatorio ya que estamos tomando la función de hash como un oraculo aleatorio). La prueba entonces sería simplemente el valor del que se tiene que tomar el módulo al utilizar la VK (clave pública).

$$Eval(SK, X) = (H(Firma(X)), N)$$

Finalmente, para implementar Verify, vamos a utilizar las propiedades de las firmas digitales:

$$Verify(VK, X, Y, \pi) = (Y == H(X^{VK} mod \pi))$$

4. **The *Ouroboros* protocol.**

   (a) (5 points) We saw in class that in the Ouroboros protocol the slot leader election process is abstracted out and modeled as an "ideal functionality." Describe one realistic approach to elect the slot leader, and explain why there are $\perp$ symbols in the characteristic strings.

   Solution: La abstracción de ideal functionality es buena para entender el protocolo, sin embargo, en la práctica, se debe usar algo aleatorio para poder elegir el slot leader. Para esto se podría aprovechar algo como las VRF y su propiedad de ser verificabemente impredecibles para seleccionar un líder de forma segura. El símbolo $\perp$ es utilizado para representar un slot en el que no se eligió a ningún líder. Es necesario ya que la elección es probabilistica y podría no elegirse a ningún minero.

   (b) (5 points) Describe the implementation of the *dynamic* stake setting. Why can't the parties use the most recent stake distribution (i.e., the stake distribution at the end of the previous epoch)?

   Solution: Queremos limitar la variación en la distribución de stake para que no varíe abruptamente de un momento a otro, permitiéndole a los mineros estimarla con la distribución de los anteriores slots. Se asegura que se mantiene un $(1/2 + \epsilon + \sigma)$ del stake en mineros honestos y la variación en la distribución es de máximo σ en un periodo determindo de R slots. En una configuración con delay de 2R esto garantiza la seguridad. Fuente: página 10