**Objetivo:** incluir en cada bloque un timestamp, dicho timestamp tendría un margen de error marcado por el CGGTTS. Esto ayudaría a facilitar el consenso y a reducir los forks. Permitiría reducir el tiempo de PoW manteniendo el consenso.

**Problema actual:** el algoritmo R2CGGTTS genera la trazabilidad a UTC, sin embargo (i) ¿cómo nos aseguramos que se ejecuta el algoritmo R2CGGTTS y no otro corrupto para obtener unos resultados mejores? (ii) aunque se ejecute el algoritmo R2CGGTTS correcto, ¿cómo estaríamos seguros de que el timestamp que se le da al bloque no es uno menor para conseguir ventaja?

**Solución(?):** en algún momento Javier habló de que debería haber una cajita (hardware) que hiciese esto. Se lleva a hardware y esta lleva un log que demuestre que todo se ha hecho de manera honesta. Aquí me pierdo, necesito que Javier me aclare si esto se puede hacer y cómo. Hablar con él sobre SGX de Intel (el utilizado en PoET).

**Remark I:** en caso de conseguirlo, el timestamp no lo puede llevar implícito el bloque ya que el timestamp marca cuándo se ha conseguido el hash del bloque buscado. La prueba para el resto de peers debería de ser un timestamp al hash final del bloque.

**Remark II:** en el caso de tener que utilizar hardware específico, recordar que, aunque pueda parecer una barrera de entrada grande actualmente ya utilizan ASICs muy costosos. Además, el PoW se encuentra actualmente bastante estancado, si se consigue un hardware que consiga mejorar la escalabilidad considero que las minning pools estarían dispuestas a usarlo. En el caso de una minning pool no sería necesaria una de estas “cajitas” para cada ASIC de su pool, con una cajita para toda la pool sería suficiente.

**REMARK III:** no olvidar lo que me dijeron Fajardo y Alfonso (Alastria), es muchísimo mejor algo semi-descentralizado que centralizado. De hecho, consideraban que para ellos algo semi-descentralizado era lo óptimo. Fajardo ya ha mencionado varias veces que para su cripto hay muchas papeletas para la semi-descentralización. Con semi-descentralizado me refiero a que se utilicen “Master nodos”.