¿Qué tipo de Blockchain necesito?

Un diagrama de flujo puede ayudar[1]

Si bien algunos de los siguientes conceptos serán explicados someramente, suponemos que el lector comprende aspectos básicos sobre *blockchain permisionada*, *no permisionada*, *pública*, *privada*, *throughput*, *latencia*, *proof of work*, *proof of stake* y *byzantine fault tolerance*.

A través de un diagrama de flujo trataremos de ayudarlo a decidir si necesita o no Blockchain para el caso considerado. De necesitarla, intentaremos asistirlo para definir el **tipo** de blockchain más adecuado: pública o privada, permisionada o no.

En general, usar una **Blockchain permisionada** solo tiene sentido cuando múltiples entidades que desconfían mutuamente desean interactuar y cambiar el estado de un sistema, sin necesidad de un tercero de confianza.

Para facilitar el proceso de toma de decisiones proporcionamos un **diagrama de flujo** en la **Figura 1**. Para él consideramos uno o varios participantes que inciden en el estado del sistema. Un **escritor** corresponde a una entidad con privilegios de acceso y escritura en un sistema de base de datos típico o un participante en el consenso de un sistema de Blockchain.

Si sólo existe un escritor, una Blockchain no proporciona garantías. Una **base de datos clásica** es más adecuada, porque proporciona un **mejor rendimiento** en términos de throughput y latencia. En criptografía, un **tercero de confianza** es una entidad que facilita las interacciones entre dos partes que confían en el tercero. Si un **tercero de confianza** (*TTP, Trusted Third Party*) está disponible, hay dos opciones:

Primero, si el TTP está siempre en línea, las operaciones de escritura se le pueden delegar y funciona como **verificador** para las transiciones de estado. Segundo, si el TTP está generalmente fuera de línea, puede funcionar como una autoridad de certificación en una Blockchain **permisionada**, donde todos los escritores del sistema son conocidos. Si todos los escritores confían mutuamente, es decir, suponen que no hay participantes maliciosos, **una base de datos con privilegio de escritura compartido** es probablemente la mejor solución. Si no confían entre sí, tiene sentido usar una Blockchain permisionada.

Si se requiere **verificación pública** y cualquiera puede leer el estado estamos frente a una **blockchain pública permisionada**. Si el conjunto de lectores está restringido es el caso de la **Blockchain privada permisionada**. Si el conjunto de escritores no es fijo ni es conocido por los participantes, como es el caso de muchas criptomonedas como Bitcoin, una **Blockchain no permisionada** es una solución adecuada.

En la **Tabla 1** contrastamos algunas propiedades de Blockchains permisionadas, no permisionadas y una **base de datos centralizada**. Esta última tiene un rendimiento (en términos de latencia y throughput) **mucho mejor** que las Blockchains, ya que ellas agregan complejidad adicional a través de su mecanismo de consenso.
Por ejemplo, Bitcoin tiene un rendimiento de aproximadamente 7 transacciones por segundo (que podría ser extendido a aproximadamente 66 sin comprometer la seguridad), mientras que un sistema centralizado como Visa puede manejar picos de más de 50.000 transacciones.
Hay un compromiso entre **descentralización**, es decir, qué tan bien un sistema escala a una gran cantidad de escritores sin confianza mutua, y el **throughput**, es decir, cuántas actualizaciones puede manejar un sistema en un período determinado. Al tomar la decisión de usar una blockchain o no debería tenerse en cuenta este compromiso.[2] [3]

---

[1] https://eprint.iacr.org/2017/375.pdf, visitado el 11/05/18

[2] What Blockchain Means for Government, http://www.gartner.com/webinar/3873165, visitado el 20/06/18

[3] https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business/, visitado el 20/06/18

	Blockchain NO permisionada	Blockchain permisionada	Base de datos centralizada
Throughput	Bajo	Alto	Muy alto
Latencia	Lenta	Media	Rápida
Cantidad de lectores	Alta	Alta	Alta
Cantidad de escritores	Alta	Baja	Alta
Cantidad de escritores no confiables	Alta	Baja	0
Mecanismo de consenso	Mayormente PoW, algunos PoS	Protocolos BFT	Ninguno
Administración central	No	Sí	Sí

Nota: **PoW** (Proof of Work); **PoS** (Proof of Stake), **BFT** (Byzantine Fault Tolerance)

FIGURA 1