La revolución de los Smart Contracts

En el presente post voy a tratar un tema que hasta el momento no lo he mencionado debido a que lo estaba reservando para el último post. Se trata de los famosos “smart contract”.

Para entender un smart contract primero hemos de recordar que significa un contrato. Un contrato no es más que un acuerdo entre dos o más partes, un entorno donde se define lo que se puede hacer, cómo se puede hacer, qué pasa si algo no se hace… Es decir, unas reglas de juego que permite, a todas las partes que lo aceptan, entender en qué va a consistir la interacción que van a realizar.

Hasta ahora los contratos han sido documentos verbales o caros documentos escritos, sujetos a las leyes y jurisdicciones territoriales, y en ocasiones requiriendo de notarios, es decir, más costes y tiempo. Algo no accesible para cualquier persona. Y esto no es lo peor, los contenidos de los contratos pueden estar sujetos a la interpretación.

En cambio un contrato inteligente es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores. Evitan el lastre de la interpretación al no ser verbal o escrito en los lenguajes que hablamos. Los smart contracts son “scripts”, siendo los términos del contrato puras sentencias ycomandos en el código que lo forma.

Por otro lado, un smart contract puede ser creado y llamado por personas físicas y/o jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma. Un smart

contract tiene validez, sin depender de autoridades, debido a su naturaleza: es un código visible por todos y que no se puede cambiar al existir sobre la tecnología blockchain, la cual le da ese carácter descentralizado, inmutable y transparente.

Si juntamos los principios de un smart contract con la creatividad de muchos desarrolladores del planeta, el resultado son posibilidades jamás vistas, accesibles para todos y a costes que rozan la gratuidad.

Imagina un coche Tesla auto-conducido, comprado en grupo, capaz de autogestionarse y alquilarse por sí solo pero sin una compañía tipo Uber detrás llevándose el 10%. Bienvenido al mundo de los contratos inteligentes.

Según Deloitte, tal y como indica en su artículo "getting smart about smart contracts" [1], los smart contract aportan numerosos beneficios en comparación con las metodologías utilizadas hasta el momento. Pero, de entre todos los beneficios destaca los siguientes:

Actualizaciones en tiempo real	Debido a que los contratos inteligentes usan software para automatizar tareas que normalmente se realizan a través de medios manuales, pueden aumentar la velocidad de una amplia variedad de procesos comerciales.
Mayor precisión	Las transacciones automatizadas no solo son más rápidas, sino que son menos propensas a errores manuales.
Menor riesgo de ejecución	El proceso de ejecución descentralizado elimina virtualmente el riesgo de manipulación, incumplimiento o errores, ya que la ejecución de la gestión se realiza automáticamente por la red en lugar de forma individual.
Menor costo	Los nuevos procesos habilitados por los contratos inteligentes requieren menos intervención humana y menos intermediarios y, por lo tanto, reducirán los costos.

Menos intermediarios	Los contratos inteligentes pueden reducir o eliminar la dependencia de terceros intermediarios que brindan servicios de «confianza», como el depósito en garantía entre contrapartes.

Una vez explicados los smart contracts voy a comentar un caso de auditoría. Un caso de auditoría de smart contract. Pero antes, os dejo un video corto que explica que es y cómo funciona un smart contract, para todos aquellos que no lo hayáis acabado de entender.

He encontrado un artículo de Merunas Grincalaitis, experto en Ethereum (una criptomoneda basada en la tecnología blockchain). Que tras centrar sus esfuerzos en aprender todo lo posible sobre auditar smart contracts con el fin de encontrar brechas de seguridad, nos expone los pasos a seguir si queremos auditar un smart contract.
Según Merunas Grincalaitis, el resultado de dicha auditoría constara de los siguientes puntos:

-Liberación de responsabilidad: Aquí se expone que la auditoría no es un documento legalmente vinculante y que no garantiza nada.

-Descripción general de la auditoría y buenas características: Una vista rápida del contrato inteligente que se auditará y buenas prácticas encontradas.

-Ataques realizados al contrato: En esta sección hablará sobre los ataques realizados al contrato y los resultados. Solo para verificar que es seguro.

-Vulnerabilidades críticas encontradas en el contrato: Problemas críticos que podrían dañar gravemente la

integridad del contrato.

-Vulnerabilidades de media gravedad encontradas en el contrato: Aquellas vulnerabilidades que podrían dañar el contrato pero con algún tipo de limitación. Como un error que permite a las personas modificar una variable aleatoria.

-Vulnerabilidades de baja gravedad encontradas en el contrato: Esos son los problemas que realmente no dañan el contrato y podrían existir en la versión implementada del contrato.

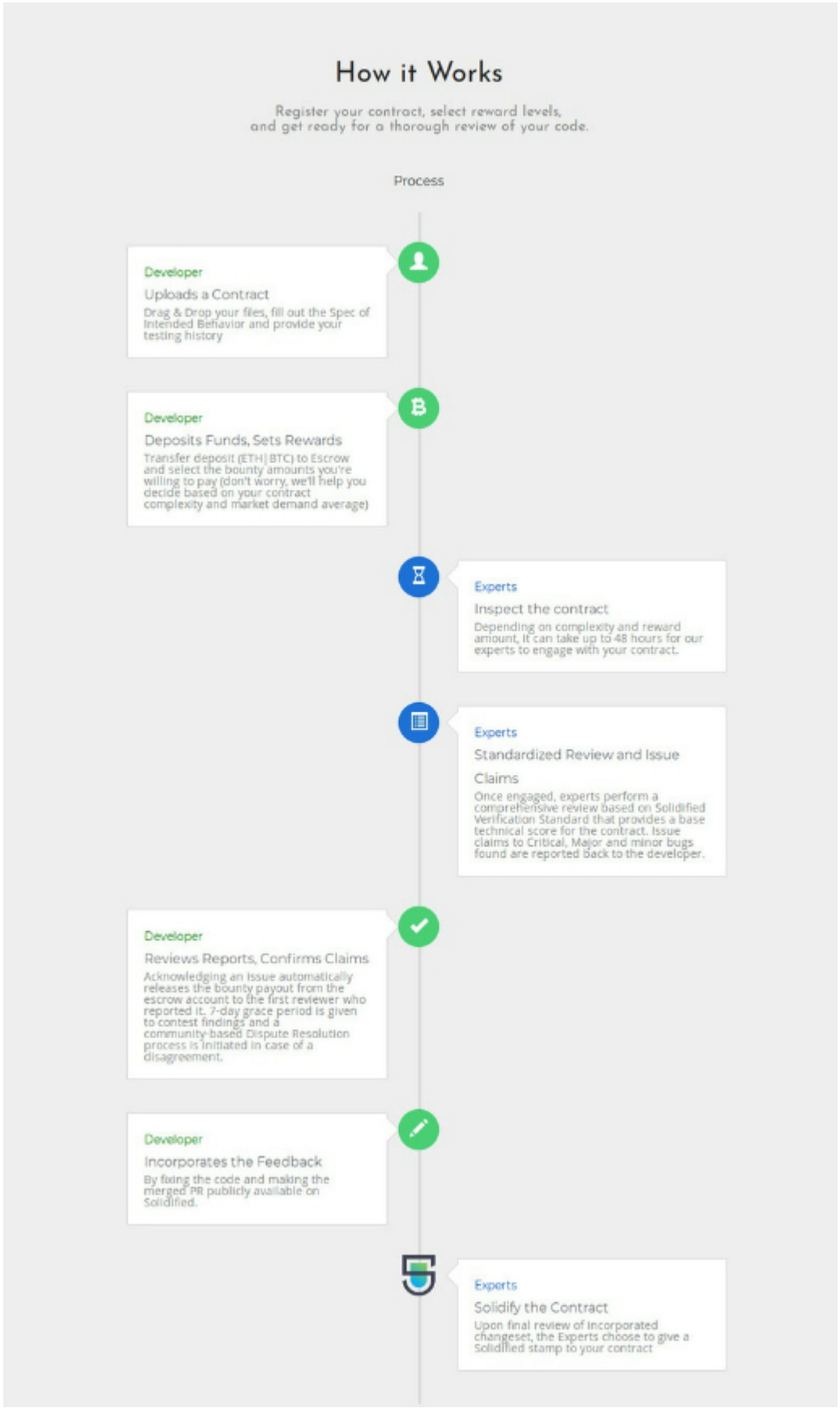
-Comentarios línea por línea: En esta sección analizará las líneas más importantes en las que verá posibles mejoras.

-Resumen de la auditoría: Su opinión sobre el contrato y las conclusiones finales sobre la auditoría.

Para interesados, en el siguiente link pone en práctica lo comentado [2], en el que audita un smart contract de un casino de Ethereum. El código del smart contract ,o podéis encontrar en su Github.

Dejando a un lado a Merunas Grincalaitis, me gustaría destacar la plataforma Solidified. Una plataforma para la revisión colectiva de contratos inteligentes, en la que cualquier desarrollador puede presentar su contrato para una revisión exhaustiva de la calidad con nuestra gran red de expertos de blockchain verificados. [5]

Donde funcionan de las siguiente manera:



En conclusión, los smart contracts son otra consecuencia del blockchain. Una consecuencia que viene para quedarse y que, sin duda alguna, va a revolucionar el mundo. Porque, cuando

los smart contracts estén estandarizados, ¿vamos a necesitar notarios? o ¿por qué un persona física que traba en un banco va a tener acceso a todos nuestros datos personales si solicitamos un préstamos? Con un smart contrat este proceso sería automático y sin violar nuestra intimidad. El susodicho banco debería estipular unas condiciones (un mínimo de X€ ahorrado, una nómina con Y€ como mínimo…) y simplemente debe saber si el cliente lo cumple, no necesita saber si tienes una nómina de 25.000€ o de 100.00€. Y como estos dos ejemplos, me vienen miles a la cabeza…

Referencias:

[1]: Getting smart about smart contracts, Deloitte (junio 2016) https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-cfo-insights-getting-smart-contracts.pdf

[2]: how to audit a smart contract, por meruna sgrincalaitis, visto el 25/11/2017, https://medium.com/@merunasgrincalaitis/how-to-audit-a-smart-contract-most-dangerous-attacks-in-solidity-ae402a7e7868

[3]: Github.com, visto el 25/11/2017, https://github.com/merlox/casino-ethereum

[4]: solidified.io, visto el 25/11/2017, https://www.solidified.io/