CURSO
BLOCKCHAIN

Modulo 4

Smart Contracts (Parte 2)

CURSO BLOCKCHAIN

Lo visto

Estudiamos:

- **web**: dApps, Web1, Web2, Web3. (15')
- **Oraculos** (5')
- **Smart Contract:** Ethereum, EVM, patriccia merkle tree, variables de estado, programa (codigo), transacciones, gas, caracteristicas, casos de ejemplo, canal de pagos, DAO (Governanza y votacion -> España) (1hs)
- Programación de uno en tiempo real (ERC20 + con contrato legal). (10’)

CURSO BLOCKCHAIN

Lo que veremos

Hoy Estudiaremos:

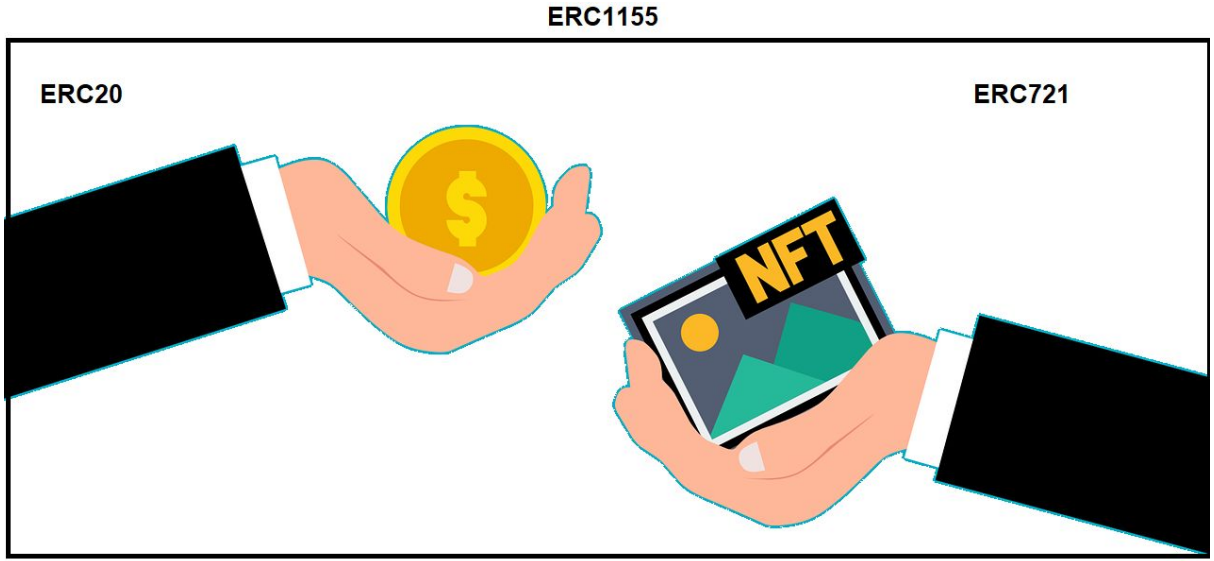
1. **Token:** criptomonedas vs token, Clasificacion por fungibilidad (ERC20, ERC721), Clasificacion por usabilidad (Utility, security,...). (50')
2. **Seguridad:** En desarrollo (Importancia, testing, Auditorías, Responsabilidad), de usuarios (Contratos maliciosos, Scammers (dust tokens, Bots de frontruning falsos, personificaciones de websites))... Mostrar alguna SCAM. (50')
3. **Hackeos:** Ronin, Tornado Cash, analisis empresarial, KYC. (20')

CURSO BLOCKCHAIN

Criptomoneda vs Token

Fungibilidad

Articulo 232 Código civil: Son cosas fungibles aquellas en que todo individuo de la especie equivale a otro individuo de la misma especie, y pueden sustituirse por otras de la misma calidad y en igual cantidad.



Usabilidad

Token de utilidad: Herramienta para que los holders participen en la gobernanza. Te brindan herramientas de utilidad pero que son dadas por la misma empresa que la emite y no algo realmente de vinculación legal. Son más fáciles para intercambiar en un mercado paralelo. (ERC20) ITO/ ICO

Security token: Contrato que significa control sobre una inversión legitima en la que un activo es utilizada como colateral. Pero la persona no tiene Control sobre ello más que las ganancias. Estos son regulados. (ERC1400 - ERC1404) STO

Equity token: Contrato que te brinda parte de una compañía. Estos son regulados. Hoy en día no hay diferencia entre los protocolos de estos y los securities.

Prueba de Howei

- Invertiste dinero?
- Esperas un beneficio?
- Invertiste en una compañía común?
- Las ganancias son dependientes de un agente externo?

Si la respuesta es si: Estamos ante un Security.

Algunas legislaciones

Estonia: EFSA (Estonian Finantial Supervisory Authority) Reconoce bajo su ambito de control aquellos que se ofrecen publicamente y representan bienes negociables. https://www.legalico.io/estonia/

Suiza: FINMA (Finantial market supervisory Authority). Para las ICOs, ellos diferencian los activos virtuales entre token de utilidad, token de pago y tokens de activos. Encuadran a las criptomonedas como un token de pago.
https://www.iosco.org/library/ico-statements/Switzerland%20-%20FINMA%20-%20ICO%20Guidelines.pdf

Argentina: Marco regulatorio de ofrecimiento (Ley 26831: oferta a publico general, usando medios masivos de comunicación y para operar valores negociables. Para solventar esto se usa oferta privada), herramienta juridica para vincular token con la cosa (Articulo 1693 del codigo civil y comercial que posibilita que un fideicomiso financiero pueda emitir o respaldar titulos de valores atipicos). Un intercambio del token será una cesión de derechos entre privados y el fiduciario velar por las normativas vigentes (KYC y AML) convirtiendo en la blockchain en una herramienta y no con el fin anarquista para el que fue creada.

España: Prohíbe la toma de decisiones mediante un tratamiento automatizado de los datos del interesado del que deriven consecuencias jurídicas . Pero podría verse desplazada por la autonomía de la voluntad. en el artículo 1.278 del CC y el 51 del Código de Comercio (CCo) se consagra la voluntad de forma siempre que concurran los requisitos del 1.261 y, salvo que se trate de los supuestos observados en el 1.280, el hecho de que el acuerdo se plasme completamente de manera criptográfica no ha de suponer impedimento para que se consideren contratos legalmente válidos. El no expresarse en un lenguaje comprensible para la mayoría no implica que no poseamos máquinas o expertos que los puedan traducir

Seguridad

1. Una vez deployado un smart contract no puede ser modificado. Un error en la codificación puede generar pérdidas muy grandes de dinero.
2. Para evitar errores se realizan testing muy rigurosos de su funcionalidad.
3. Es importante que sean auditados (Openzeppelin, Consensys, Coinfabric).
4. ¿Cual es la responsabilidad del desarrollador y cual de usuario?

CURSO BLOCKCHAIN

Contrato Malicioso

Dust Token

Encargado de destruir anonimicidad de Bitcoin

1. Envío algunos satoshis a muchas wallets
2. Escucho cuando se manda esa transacción
3. Vinculo las address que conformaron el capital envíado como una.
4. Busco información sobre cualquiera de ellas y obtengo al dueño del address.

Evitarlo:

1. Tener cuidado con la información personal que se dá por internet.
2. Guardar montos grandes en wallets frías para que tengan la menor exposición posible.

Air Drops

Formas:

1. Envío token gratis a la gente.
2. Agrego un poco de liquidez en un DEX importante para que piensen que vale cierto dinero pero sin demasiada liquidez.
3. Los redirigo a mi dApp.
4. Una vez que quieren hacer el swap, el contrato que les hago firmar no es del swap sino que les pido permiso para mover los activos de su wallet.
5. Extraigo todos sus fondos.

Evitarlo:

1. Tener cuidado con los air drops. Nadie regala dinero gratis.
2. Utilizar solo sitios confiables para los swap, en casos de sitios nuevos solo si son capaces de entender los contratos y saber que están firmando.
3. Usar billeteras con lo justo y necesario para conectarse a sitios nuevos.

Información falsa:

1. ~~Desconectarme del sitio le quitá la posibilidad de seguir sacandome dinero.~~

Personificación de websites

Forma:

1. **Hago un sitio muy similar a una existente.**
2. **Al firmar contrato en realidad le pongo mi contrato malicioso**
3. **Le extraigo todo el dinero.**

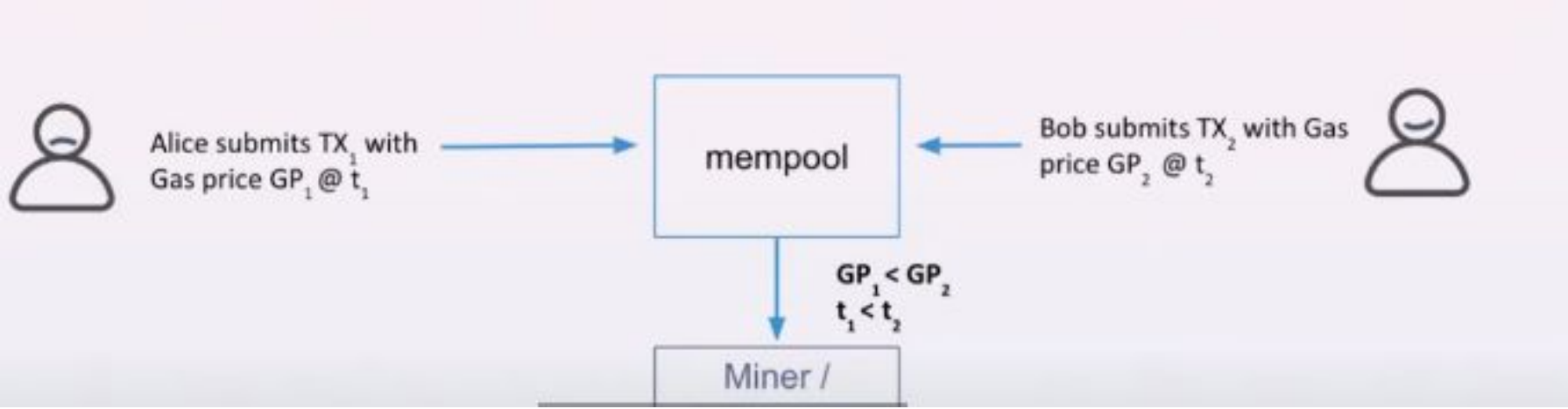
Forma 2: Igual que antes pero atacando la web para cambiarle el smart contract que firma.

Forma 3: Igual que antes pero el cambio se lo hago local al usuario mediante una extensión maliciosa.

Evitarlo:

1. **Verificar que la url sea la correcta.**
2. **Verificar certificados SSL**
3. **Verificar Smart contract que estoy firmando.**

Bots de frontruning



CURSO BLOCKCHAIN

Tornado Cash

Hackeo Ronin

Ataque 51% perpretado por:

0x098B716B8Aaf21512996dC57EB0615e2383E2f96

Opinión

¿Marcó un antes y un después respecto al libre uso lo sucedido con tornado cash?

¿Como piensan que eso pueda actuar como jurisprudencia para el futuro?

Análisis Empresarial

¿Cómo piensan que esta tecnología pueda ser utilizada en el ámbito empresarial?

¿Qué cosas pueden aplicarse en el ámbito jurídico?

¿Que ven que no pueda confluir nunca?

¿Que ven que pueda estar bueno si se implementara?

Bibliografía

1. Mastering Ethereum, Andreas Antonopoulos
2. Token vs criptomonedas: https://www.bbva.com/es/innovacion/que-diferencias-hay-entre-un-token-y-una-criptomoneda/
3. Security, equity y utility token: https://medium.com/security-token-offering/security-token-development-company-blockchain-app-factory-f5481ffec676#:~:text=The%20key%20difference%20between%20Security,company%20are%20diluted%20into%20tokens.
4. security tokens: https://www.securities.io/equity-tokens-vs-security-tokens/
5. Regulación Security token: SECURITY TOKEN OFFERINGS: REGULATORY GAPS IN EXISTING EU FINANCIAL SERVICES REGULATION, James Camilleri, faculty of Laws, University of Malta , September 2020

Bibliografía

6. Noticia sobre evasión de la sec con security tokens: https://www.securities.io/gladius-dodges-a-blow-from-the-sec/
7. Marco legal para la tokenización en argentina: http://sedici.unlp.edu.ar/handle/10915/132611
8. Noticia tornado cash: https://www.forbesargentina.com/money/el-caso-tornado-cash-genera-descalabro-mundo-crypto-n20238
9. Noticia Ronin bridge: https://es.cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack
10. Regimen juridico y problematica de los smart contracts (Universidad de zaragosa): https://core.ac.uk/download/pdf/289997637.pdf

Resumen

1) **Cryptomoneda:** Activo digital utiliado para el mantenimiento de una red y que sirve como unidad de intercambio.
2) **Token**: Ficha que representa otra cosa. Puede ser fungible o no fungible y el registro queda en la blockchain como un libre contable inalterable por las características que estudiamos. Podemos dividirla en utility o securities según su uso y el test de howei.
3) **Seguridad en blockchain**: Por más que la blockchain es abierta a todo el mundo está pensada para un público capaz de entender lo que firma. Igual que legalmente no podemos adjudicar desconocimiento de la ley, acá tampoco pero las consecuencias son inmediatas sin un intermediario como sería el caso de un juez. Todo el mundo es así realmente pero acá el 90% de las veces entra en juego dinero.
4) **Hackeos**: Estos se dan por ingeniería social, No es redituable hackear una blockchain salvo que sea una sidechain como lo era Ronin relativamente sencilla de hackear, pero el acceso también se obtuvo por ingeniería social ya que la criptografía es sumamente segura.
5) **Legalidad**: Si bien todo es un camino gris han habido varios intentos internacionalmente de enmarcar las actividades utilizando la blockchain.

Consultas

¿?

Reto

https://cursoblockchain.com.ar/

Actividad

a) El algoritmo pensado la clase pasada. ¿Cómo se lo podría violentar y no conseguir los resultados queridos?
b) ¿Cómo podemos solventar o crear algún acto que reduzca el riesgo de la falla del smart contract anterior?
c) ¿Cómo piensan que podrían aplicar los smart contracts en su vida profesional diaria?