Universidad Abierta Interamericana

Sistema de Penalización basado en Datos Biométricos y Blockchain para Videojuegos

Tutoría técnica: Ing. Pablo Vilaboa

Profesora de trabajo final: Dra. Marcela Samela

Alumno: Kevin Miyashiro

CIITI – Congreso Internacional en Innovación Tecnológica Informática

1 de Septiembre, 2023

Resumen

En el presente paper se explicarán los fundamentos de la solución conceptual que se ofrece en el marco del Trabajo Final de Carrera de la Licenciatura en Gestión de Tecnología Informática para la Universidad Abierta Interamericana, llamado Sistema de Penalización basado en Datos Biométricos y Blockchain para Videojuegos. Este trabajo tiene como objetivo ofrecer un sistema alternativo frente a las penalizaciones que se determinan sobre los usuarios que infringen las normas en los videojuegos online para obtener una ventaja ilegítima sobre los demás usuarios, ocasionando un ambiente hostil en toda la comunidad.

Este inconveniente se ha presentado de manera reiterada desde el origen de los videojuegos online, sin poder lidiar con ello de raíz, y generando pérdidas económicas para las empresas propietarias. Esta propuesta de intervención en el campo profesional busca complementar a los sistemas antitrampas actuales, centrándose en las sanciones hacia los usuarios reales de manera definitiva, con el fin de mantener la comunidad limpia. Por tal motivo, en primer lugar, se explicará qué son las trampas en los videojuegos, como también así los diferentes sistemas antitrampas actuales y las penalidades que se aplican sobre los usuarios por infringir las diferentes normas. Luego se expondrán los diferentes conceptos de Blockchain, centrándose en los sistemas parcialmente descentralizados y en los contratos inteligentes (Smart-Contracts). Además, se utilizará la Biometría que servirá de base para obtener los datos de los usuarios de forma unívoca.

Se propone implementar un sistema de penalización parcialmente descentralizado que permita el almacenamiento de los datos biométricos, utilizando la tecnología Blockchain.

Es importante destacar que lo mencionado en este paper hace referencia a una propuesta de intervención en el campo profesional, en la que el autor aún se encuentra trabajando y no ha sido finalizada.

Palabras clave: *antitrampas, biometría, blockchain, penalizaciones, videojuegos.*

Abstract

The following research paper will explain the foundation of the final degree in computer science project for the Interamerican Open University which is named Punishment System based on Biometrics Data and Blockchain for Videogames. The objective of this project is to offer an alternative system when facing punishments for cheaters in videogames. These users gain an illegal advantage against the rest of players making a really bad environment for the whole online gaming community.

Nowadays this problem stills happens frequently generating company economic losses and without having a solid solution to solve it. To keep the community clean this solution proposal looks for complementing current anti-cheat systems and focusing on real user punishments in a permanent way.

First, it will be explained what a cheat is in videogames. Then the different types of existing anti-cheat systems will be seen and which penalties are applied to cheaters for violating game rules. After introducing the mentioned concepts Blockchain including partially decentralized systems and smart contracts will be exposed. Biometry will help to identify users and to obtain characteristics that are unique to an individual.

It is proposed to implement a partially decentralized punishment system based on Blockchain technology that allows biometrics data storage.

It is important to mention that what is written in this research paper is related to a solution proposal in which the author is currently working on it and it has not finished yet.

Keywords: *anti-cheat, biometry, blockchain, punishments, videogames.*

Descripción del problema

En la actualidad los propietarios del software de videojuegos online son amenazados constantemente por los usuarios que presentan un comportamiento tramposo (Duh y Chen, 2009, p. 567), obteniendo cierta ventaja ilegítima sobre los demás usuarios. Esto afecta negativamente a toda la comunidad de videojuegos online.

Según Lehtonen (2022), cuando los usuarios perciben la presencia de numerosos usuarios tramposos, la jugabilidad se degrada a tal punto, que muchos de los usuarios deciden finalmente abandonar el juego u optar por jugar un juego de la competencia. El punto más importante por destacar es el problema que deben afrontar los stakeholders, debido a que perder usuarios en la plataforma, se traduce en grandes pérdidas económicas y deriva en un serio impacto en el negocio. Por lo mencionado anteriormente, es que se debe tener especial cuidado con este aspecto, para asegurar la continuidad del producto software y de la compañía en el tiempo.

Existen múltiples investigaciones acerca de las diferentes trampas que realizan los usuarios en los videojuegos, de los sistemas antitrampas actuales y también del comportamiento de los individuos en este mismo ámbito (Consalvo, 2007). Sin embargo, poco se habla de las penalizaciones, y más específicamente de la efectividad de cada una.

Hoy en día se dispone de diferentes métodos para sancionar a las personas que realizan trampa al jugar videojuegos en línea. Entre los que podemos enumerar la desconexión de la sesión del usuario, la suspensión de cuenta (permanente o temporal), el bloqueo de dirección IP, y el bloqueo de dirección MAC (prohibición por hardware), entre otros. (Van de Ven, 2023, p 17)

Todos estos métodos pueden ser implementados por las empresas propietarias del software, por los desarrolladores de los videojuegos o por empresas terceras desarrolladoras de software a través de un sistema antitrampas. Por ejemplo, a través del Valve Anti-Cheat System (VAC) (Valve Corporation, s.f), con el Riot Vanguard (Riot Games, 2020), o mediante el Easy Anti-Cheat (Epic Games, 2023).

Los sistemas antitrampas mencionados se encargan de forma automática de la prevención, detección y penalización de los usuarios tramposos, ofreciendo diferentes escenarios como la implementación del sistema del lado del cliente o en el servidor (Van de Ven, 2023, p 7).

Si bien cada tipo de sanción ofrece diferentes ventajas, lo que tienen en común los métodos mencionados es que permiten de alguna manera la reincidencia de los usuarios infractores. Basta con crearse una cuenta nueva, cambiar la dirección IP utilizada, conseguir un nuevo hardware o computadora y volver a conectarse, para continuar haciendo uso del software o jugar de forma ilegítima.

Justificación de la propuesta

La propuesta de intervención busca ser un complemento a los sistemas antitrampas actuales. Sin ánimos de reemplazarlos, debido a que en primer lugar estos sistemas antitrampas deberán detectar a los usuarios infractores, para luego ser reportados en un sistema parcialmente descentralizado (Zheng et al., 2017, p 559). Buscando desalentar cualquier actividad en los usuarios que esté relacionada estrechamente con el uso de trampas, el uso de software de terceros, la explotación de bugs, o cualquier otro aspecto que permita obtener una ventaja ilegítima en el videojuego, sobre el resto de los usuarios.

El sistema de penalización parcialmente descentralizado resguardará los datos biométricos de todos los usuarios de las plataformas adheridas y contará con información adicional acerca de los antecedentes. El conjunto de esta información será oportuno y de utilidad para la toma de decisiones de los stakeholders, asegurando la continuidad del producto software, manteniendo a los usuarios activos y evitando posibles pérdidas económicas.

El hecho de que un usuario sea reportado en esta plataforma implica que todas aquellas entidades que se encuentren vinculadas a este consorcio, disponen de información acerca del usuario. De esta forma, las empresas asociadas a este sistema podrán consultar el historial de las personas y si

han sido marcados por otro sistema antitrampas en el pasado, en otras palabras, si los usuarios han realizado algún tipo de trampa. En caso afirmativo, los propietarios del software podrán reservarse el derecho de admisión de los usuarios en su plataforma.

Marco Institucional

Este trabajo está destinado principalmente a las empresas desarrolladoras de videojuegos y a otros stakeholders, que busquen frenar el abuso por parte de los usuarios tramposos y de mantener la comunidad limpia.

Objetivos Generales y Específicos

Objetivo General

Proponer un sistema de penalización parcialmente descentralizado para los videojuegos online, basado en la tecnología Blockchain y en el resguardo de los datos biométricos.

Objetivos Específicos

Para poder satisfacer el objetivo general, será necesario cubrir los siguientes aspectos:

- Indicar cómo el sistema se integrará a los sistemas antitrampas actuales.
- Presentar un plan para implementar el sistema de penalización.
- Explicar las limitaciones que dificultarían la implementación y el funcionamiento de la propuesta mencionada.
- Promover a los stakeholders a adoptar este sistema basado en Blockchain, para reportar y castigar de forma permanente a usuarios conflictivos.
- Desalentar a los usuarios a realizar trampas en los videojuegos online.

Contribuciones Principales

Esta propuesta brindará una herramienta para mantener la comunidad limpia, ayudando a los propietarios del software a detener a los usuarios tramposos, y minimizando el impacto en el negocio por las posibles pérdidas económicas.

Implementar este sistema, resultará en un espacio colaborativo en el que diferentes empresas podrán apoyarse mutuamente para lidiar con este tipo de usuarios.

¿Qué se considera Trampa o Cheat en los videojuegos online?

Hoy en día la mayoría de las personas optan por jugar en línea, en comparación a como lo era en el pasado, que solamente competían contra la computadora (contra la “IA” o inteligencia artificial). Esto se debe a que las personas encuentran mucho más interesante el juego cooperativo y competitivo online, en comparación con el viejo paradigma local (Duh y Chen, 2009, p. 567). Por el motivo mencionado anteriormente, es que abordaremos los diferentes escenarios que se presentan en el ámbito online.

Cada compañía desarrolladora de videojuegos puede adoptar diferentes posturas con respecto a lo que se considera o no, comportamiento tramposo. Según Duh y Chen (2009, p. 568) esta falta de consistencia se debe a tres razones, primero que se trata de una problemática que no ha sido abordada en profundidad por los investigadores, segundo que diferentes tipos de juegos implican diferentes formas de hacer trampa, y tercero que nuevas trampas son desarrolladas en el momento que los sistemas antitrampas logran neutralizar a las anteriores. Por otro lado, los jugadores se ven influenciados por diferentes factores subjetivos y por sus propios valores para definir el concepto de trampa (Consalvo, 2007, p. 87).

En este trabajo en particular vamos a considerar como trampa, a cualquier uso de software externo, modificación del software cliente o servidor para obtener una ventaja desleal sobre el resto de

los jugadores, como también así cualquier aprovechamiento de alguna falla en el software (*bug*) o manipulación de la red. El tipo de trampa más conocido por los usuarios es el uso de software externo, que permite modificar el comportamiento del cliente del juego en cuestión. Del punto de vista técnico, hay dos elementos computacionales que se pueden manipular con estas herramientas: la memoria RAM *(Random Access Memory*) o la red. (Van de Ven, 2023, p. 6).

La relevancia de cada trampa, está relacionada con el tipo de juego que el usuario esté ejecutando (Lehtonen, 2020, p. 8). Por ejemplo en los juegos de disparos en primera persona (*First Person Shooters*), el llamado *wallhack*, se refiere a la modificación de las texturas gráficas del juego permitiendo ver a través de las paredes y pudiendo detectar enemigos, cuando en realidad no debería suceder. Según Chen y Duh (2009), el aumento en los reflejos, consiste en reemplazar mediante un programa o software externo, las reacciones humanas para producir resultados superiores. Un ejemplo de lo que mencionan los autores, es el *aimbot* o *aimhack*, un software que permite apuntar a los enemigos de forma automática. Por otro lado, las trampas mencionadas anteriormente, no son de gran importancia en otros juegos, como por ejemplo en los juegos por turnos. En este género de juegos, espiar la red para modificar paquetes podría ser mucho más beneficioso del punto de vista del atacante (Lehtonen, 2020, p. 9).

Además es necesario establecer un criterio de clasificación para cada una de las trampas según el impacto en la plataforma online. Según Lehtonen (2020), se establecen dos categorías para indicar el grado de severidad de las trampas realizadas por los usuarios. Se distinguen las trampas livianas y las trampas duras. Cuando se habla de trampas livianas, el autor se refiere a la manipulación de las mecánicas del juego para obtener una ventaja ilegal sobre los demás jugadores. Estas características mencionadas no han sido programadas de forma intencional por los desarrolladores del videojuego. Un ejemplo de lo mencionado anteriormente podría ser aprovecharse de un bug de forma deliberada, generar dinero dentro del juego de forma rápida por alguna falla en el software, o realizar transacciones con dinero real fuera del juego para obtener beneficios dentro, como la compra de ítems. Por otro lado, las trampas duras (*hard cheats)* son aquellas trampas por las cuales los sistemas antitrampas han sido principalmente desarrollados. Se refiere específicamente al uso de programas externos para manipular el software cliente, o a la modificación de los paquetes de red que el cliente envía al servidor. Es importante destacar que los programas externos pueden inyectarse por sí mismos en la memoria, para crear nueva funcionalidad llamando a las funciones estándar del juego.

¿Qué es un Sistema Antitrampas?

Con el fin de detener a los usuarios que buscan obtener una ventaja ilegítima sobre los demás, los sistemas antitrampas se encargan de la detección, prevención y penalización de las trampas en los videojuegos online de forma automática (Van de Ven, 2023, p 7). En la actualidad existen diferentes tipos de sistemas antitrampas, pero en general son agrupados en dos grandes categorías, los sistemas antitrampas que funcionan en el servidor (*server-side*) y los que se encuentran en el cliente (*client-side*).

Aquellos que funcionan únicamente en el servidor, se encargan de revisar los paquetes de red provenientes del cliente y aseguran que los datos y el estado del juego sean manipulados correctamente en el servidor. Por otro lado, los sistemas antitrampas que se encuentran en el cliente, operan en la computadora del usuario y envían información al servidor (Lehtonen, 2020, p. 13). Dentro de los sistemas antitrampas que se encuentran dentro del servidor, podemos enumerar la revisión de los datos enviados por el cliente, el diseño de aplicaciones utilizando un protocolo resistente a las manipulaciones, la ofuscación del tráfico de la red y el análisis de datos estadísticos.

Como regla general, es importante que el servidor no confíe ciegamente en los datos que le son enviados por el cliente del juego (Lehtonen, 2020, p. 13). De no ser así, se podría estar procesando información proveniente de un cliente modificado, con el objetivo de realizar acciones en el servidor de forma malintencionada. Es responsabilidad del servidor realizar los diferentes controles en los datos recibidos, y los desarrolladores deben tener en cuenta diferentes decisiones de diseño para que estos datos no sean manipulados. En ciertas ocasiones el cliente del juego es el encargado de procesar datos

y de determinar estados del juego, sin involucrar al servidor, si bien es cierto que evita la sobrecarga del servidor, y ciertos problemas de performance, los inconvenientes de seguridad que se producen no justifican esta característica.

Por otro lado, es importante determinar el protocolo a utilizar para el envío y recepción de datos entre el cliente y el servidor. (Lehtonen, 2020, p 19). Por un lado, TCP (*Transmission Control Protocol*) (Postel, 1981) fue diseñado para enviar datos en bloques, estableciendo una secuencialidad en los paquetes, por lo tanto, no pueden enviarse dos paquetes con la misma secuencia. Además, en cuanto un paquete no puede ser enviado, los siguientes paquetes se bloquean hasta que se envíe el paquete anterior. Esto podría resultar en un problema de performance en los videojuegos que involucran un tráfico constante entre el cliente y el servidor. En el caso de UDP (*User Datagram Protocol*) (Postel, 1980), esta secuencialidad no existe, y la lógica de control debe ser implementada por el programador. De todas formas, el protocolo TCP brinda mayor seguridad antitrampas en comparación con el protocolo UDP. Además, se debe tener en cuenta que la información que se envía en los paquetes a través de la red, debe ser la mínima necesaria para establecer ciertos estados del juego. El hecho de incluir más información de la necesaria podría dar lugar a ser manipulada por un usuario tramposo para anticipar ciertos eventos que en realidad, no debería conocerlos.

Para evitar que los paquetes que se transmiten por la red sean capturados y leídos fácilmente, es necesario establecer alguna técnica de encriptación en la información que se envía del servidor hacia el cliente. Luego el cliente deberá incluir internamente la función inversa para poder desencriptar los datos. Al concepto mencionado anteriormente, se lo denomina ofuscación del tráfico de la red mediante encriptación (Lehtonen, 2020, p. 23).

Finalmente, el análisis de los datos estadísticos es otra alternativa de sistema antitrampas en los videojuegos online que es establecida en el servidor. Consiste en la revisión de los logs generados por los diferentes eventos, que aportan información significativa para determinar si un usuario se encuentra o no realizando trampa (Lehtonen, 2020, p 28). Una de las características más importantes por destacar, es que no se trata de un método intrusivo, sino que solamente se basa en la información generada por los eventos del videojuego. Por ejemplo, en los juegos de disparos como en el Counter-Strike, se analiza la cantidad promedio de enemigos abatidos por partida, el promedio del daño recibido o realizado, y demás datos relacionados con el puntaje del jugador. El conjunto de estas variables conlleva a marcar como sospechoso a un usuario, el cual es derivado a revisión manual por parte de algún miembro del equipo de revisión. Finalmente, el encargado de analizar al usuario es quien dictamina si se trata de un tramposo, y emite un juicio en el que prohíbe o no al usuario de continuar utilizando la plataforma. Es importante tener en cuenta que para poder utilizar este método se requiere de una base de usuarios significativa, en la que sea factible evaluar las estadísticas y promedios de los valores.

Hasta ahora se han comentado los diferentes tipos de sistemas antitrampas que se ejecutan del lado del servidor, a continuación, se hará una revisión bibliográfica de los sistemas antitrampas que se encuentran del lado del cliente.

Hoy en día estos sistemas antitrampas (client-side) son los utilizados por las empresas desarrolladoras de videojuegos para detectar trampas en la computadora del usuario. Al delegar la responsabilidad de detección de usuarios tramposos al cliente, el servidor cuenta con más recursos disponibles, mejorando la performance general del servicio. El problema que presentan estos sistemas es que las revisiones de seguridad se realizan completamente en el equipo que ejecuta el videojuego, por lo tanto, un usuario experimentado podría analizar y burlar estos controles con el fin de ejecutar programas externos o realizar modificaciones en el cliente. Dentro de los métodos antitrampas que se ejecutan del lado del cliente, podemos enumerar los siguientes: encriptación del código fuente, verificación de archivos mediante la codificación criptográfica (*hash)*, la detección de trampas conocidas, y la ofuscación de la memoria (Van de Ven, 2023, p. 7). La encriptación del código fuente se refiere a disponer del cliente del juego en forma encriptada y solamente desencriptar las partes de este, a medida que el juego es ejecutado. Esto hace el programa más difícil de ser interpretado y manipulado por el usuario, aunque no imposible. La verificación de archivos mediante alguna técnica

criptográfica sirve para verificar si alguno de los archivos del cliente sufrió alguna modificación y ya no se encuentra en su estado original. Algunos usuarios podrían realizar modificaciones en el cliente del juego para cambiar bibliotecas (*DLLs*), manipular la memoria y el comportamiento del juego. Esta revisión se realiza en primer lugar en cuanto se ejecuta el juego y en caso de que el cliente detecte alguna anomalía, detendrá la ejecución inmediatamente solicitando revisar los archivos o descargar nuevamente el cliente del juego.

La detección de trampas conocidas consiste en la revisión de los procesos, la memoria RAM, y los discos locales en busca de programas externos que se encuentren del lado del cliente y que estén relacionados con la realización de trampas en los videojuegos. Es importante destacar que las empresas desarrolladoras de videojuegos, no hacen público el completo funcionamiento de sus sistemas antitrampas, para no otorgar información sensible a los hackers y demás usuarios tramposos que busquen denegar estos sistemas. Por el motivo comentado anteriormente es que los sistemas antitrampas que se ejecutan en el cliente, podrían ser intrusivos dependiendo de cada desarrollador, ya que podrían compartir más información que la necesaria, para la detección de trampas.

¿Qué son y cómo se aplican las penalizaciones en los Videojuegos?

Las penalizaciones se refieren a las medidas que toman las empresas desarrolladoras de videojuegos o el operador del juego, contra los usuarios que realizan trampas. Como hemos comentado en la introducción de este trabajo, se refiere a la suspensión temporal o permanente de las cuentas de usuarios, al bloqueo de dirección IP, a la prohibición por hardware, o a la desconexión del usuario (Van de Ven, 2023, p 17). El problema que deben afrontar los stakeholders además de las pérdidas económicas producidas por el abandono de los usuarios en la plataforma, es la reincidencia de los usuarios tramposos ya que cualquiera de los métodos anteriores puede ser evadido con facilidad. A continuación explicaremos como funciona cada una.

La suspensión de cuenta, se refiere a una prohibición temporal o permanente de acceso del usuario a la plataforma mediante un *flag* (bandera o marca), para indicar que el usuario está suspendido. Para volver a ingresar a la plataforma, los usuarios necesitan crearse una cuenta nueva asociado a otro email, o esperar a que el tiempo de penalización acabe. El bloqueo de dirección IP, se refiere a prohibir las conexiones entrantes desde cierta ubicación (IP) otorgada por el ISP (Internet Service Provider). Los usuarios pueden utilizar una VPN (Virtual Private Network) para saltar este inconveniente o solicitar al ISP para renovar esta dirección. La prohibición por hardware hace referencia al bloqueo de alguno, o de todos los componentes utilizados en la computadora origen de la infracción. La más común se refiere a la prohibición de MAC Address (Media Access Control) que identifica unívocamente a la placa de red. Finalmente la desconexión de usuario siendo la más leve, se refiere al cierre de la conexión entre el cliente y el servidor. En este último caso, es necesario reejecutar el software para hacer uso de él nuevamente.

La Tecnología Blockchain

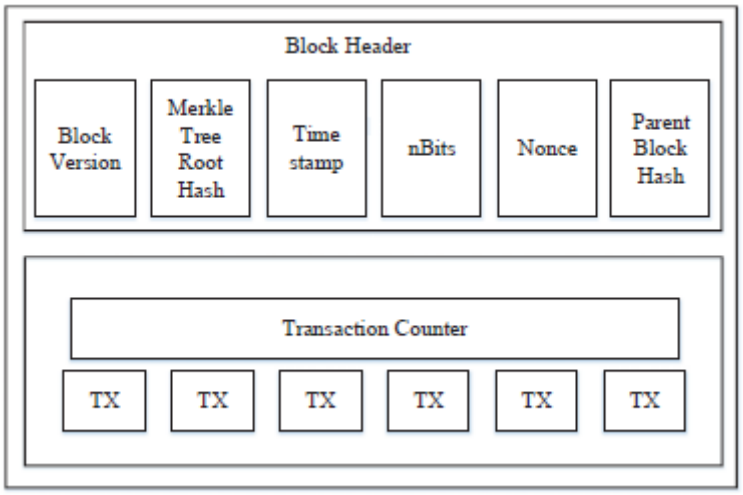
Para poder comprender cómo Blockchain puede apoyar a los stakeholders en la toma de decisiones, en primer lugar, es necesario comprender qué es y cómo funciona esta tecnología.

Por otro lado se diferenciarán los tipos de sistemas Blockchain que existen, las características y ventajas de cada uno haciendo énfasis en los sistemas parcialmente descentralizados (*cortisum blockchain*), y los contratos inteligentes que permitirán la ejecución de lógica de programación, acorde al modelo a utilizar.

En sus orígenes, el concepto de Blockchain fue introducido por primera vez como una solución entre pares (*peer-to-peer*), para poder enviar y recibir dinero sin la necesidad de la participación de un intermediario, como lo es el banco. La primera implementación de esta tecnología fue la criptomoneda Bitcoin (Nakamoto, 2008). El blockchain puede comprenderse como un gran libro contable público y distribuido, que guarda todas las transacciones asentadas en una lista de bloques. La cadena crece a medida que nuevos bloques son agregados a la misma constantemente. Las ventajas del uso de la

tecnología Blockchain está determinada por características específicas, entre las que podemos nombrar, la descentralización, persistencia, el anonimato y la auditabilidad (Zheng et al, 2017).

El blockchain puede entenderse como una secuencia de bloques. El bloque actual tiene en su cabecera el *hash* del bloque anterior, esto resulta en que cada bloque tiene solamente un bloque padre (Zheng et al, 2017, p 558). Un *hash* es el resultado de una operación criptográfica para identificar unívocamente a un bloque en particular. El primer bloque de la cadena se denomina bloque génesis, este no tiene antecesor. Un bloque está compuesto por su cabecera y su cuerpo, dentro de la cabecera podemos enumerar los siguientes componentes: la versión del bloque, el hash del árbol de Merkle, la fecha, una cantidad de bits "n", un número para una única utilización, y el hash del bloque padre. El cuerpo del bloque, está compuesto por las transacciones y por un contador.



Nota. Adaptado de Block structure, Zheng et al., 2017, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" (p. 558).

El sistema mencionado en la propuesta, se apoya fundamentalmente en que el blockchain es inmutable, esto quiere decir que cuando los bloques de transacciones son agregados al sistema, no pueden ser modificados. Aquellos usuarios reportados en este sistema quedarían marcados y podría llevarse un historial del comportamiento de cada uno, de la misma forma que un sistema de reputación. Además, la característica de la descentralización resulta en sistemas distribuidos. Esto quiere decir que la información se encuentra replicada en los diferentes nodos pertenecientes al blockchain. Por otro lado, que sea distribuido lo hace invulnerable frente a las fallas o ataques, que puedan producirse en algún nodo en particular.

En blockchain para poder establecer consenso entre los diferentes nodos sin confianza, es necesario que estén de acuerdo con respecto al protocolo utilizado para actualizar la información y mantener sincronismo en el libro contable. Este inconveniente se lo considera un problema bizantino (Zheng et al., p 559), en el que un ataque fallará solamente si ciertos generales atacan la ciudad, mientras que otros deciden no hacerlo, de forma análoga en blockchain si los nodos no llegan a un consenso mediante la validación de las transacciones, éstas no son adheridas al bloque ni a la cadena. Existen diferentes algoritmos de consenso, dentro de las más importantes podemos enumerar, PoW (*Proof-of-work*) (Nakamoto, 2008), el cual es utilizado por la blockchain de Bitcoin, PoS (*Proof-of-Stake*), como una alternativa más costo eficiente que PoW. PBFT (*Practical Byzantine Tolerance*), que es la que utiliza el framework de Hyperledger Fabric, para los sistemas parcialmente descentralizados, como los blockchain de consorcio. DPOS (*Delegated proof of stake*) que es similar a PoS, pero se trata de una democracia representativa, mientras que en PoS es una democracia directa. Ripple, que utiliza un algoritmo de consenso basado en subredes de confianza colectivas dentro de una red mayor y Tendermint que al igual que PBFT, utiliza un algoritmo bizantino de consenso (Zheng et al. 2017, p 560).

Los Sistemas Parcialmente Descentralizados

Para poder optar por un tipo de implementación blockchain, es necesario comprender primero como funciona cada una, junto con sus características específicas.

Existen diferentes tipos de implementaciones de Blockchain, cada una de ellas denotan características con respecto a la descentralización, la eficiencia, inmutabilidad, los permisos, y al mecanismo de consenso. Podemos definir tres tipos de categorías de sistemas blockchain, las públicas, las privadas y las de consorcio. En este trabajo en particular, la implementación se basará en un sistema blockchain de consorcio, en el que las empresas interesadas podrán asociarse para cooperar.

Según Zheng et al. (2017) con respecto a la taxonomía, en las implementaciones de blockchain públicas, la información se encuentra visible para cualquiera que quiera acceder a los datos, y todos pueden formar parte del proceso del consenso. Es diferente en el caso de las privadas, ya que un único ente regula el funcionamiento de la misma y solo un grupo perteneciente de nodos de cierta organización pueden participar en el proceso de consenso y de acceso a la información. Finalmente las blockchain de consorcio (*consortium blockchains*), corresponden un grupo selecto de nodos que pueden participar en el proceso de consenso y acceso a datos, pero estos nodos corresponden a diferentes organizaciones. La diferencia principal entre estos tres tipos de sistemas es que los sistemas blockchain públicos son completamente descentralizados, los privados al ser operados por una única empresa son centralizados y los de consorcio son parcialmente descentralizados, ya que un grupo de organizaciones participa de este consenso. De la misma forma los permisos de lectura también varían entre implementaciones, por ejemplo en los sistemas públicos cualquiera puede acceder a los datos, en los privados solamente los nodos pertenecientes a la organización, y en los de consorcio aquellas organizaciones que forman parte del mismo. Al hablar de inmutabilidad de los datos, es importante destacar que en los sistemas blockchain públicos resulta casi imposible manipular las transacciones, debido a la gran cantidad de usuarios que pueden participar del proceso de consenso. Por otro lado, en las privadas y de consorcio, lo mencionado anteriormente puede suceder al tratarse de un grupo reducido de nodos, en el que la mayoría decida corromperse. En cuanto a la eficiencia de cada una de las implementaciones, en las públicas se demora un gran tiempo en que las transacciones se propagan a través de la red para ser validadas debido a la inmensa cantidad de nodos que existen, resultando en una alta latencia. De forma contraria en las implementaciones privadas o de consorcio, el tiempo de propagación y validación es menor, por lo tanto se tiene una latencia baja y una mayor eficiencia.

Los Contratos Inteligentes

Con el surgimiento de la tecnología blockchain en la última década, se ha demostrado sus aplicaciones en múltiples áreas. La integración de blockchain con los contratos inteligentes, brinda gran flexibilidad para diseñar, desarrollar e implementar varios problemas de la vida real en menos tiempo y costo sin involucrar a un sistema tradicional basado en terceros (Mohanta et. al, 2018). La propuesta mencionada en este trabajo, requiere de la generación de estos contratos para poder interactuar con el sistema blockchain y actualizarlo, sin necesidad de una entidad central controladora. El concepto de contrato inteligente fue mencionado por primera vez en el año 1994 por Mark Szabo para almacenar lógica de programación de forma descentralizada.

Según Mohanta et al. (2018), un contrato inteligente es un programa informático, que puede verificarse por sí mismo, que se ejecuta automáticamente y es resistente a la manipulación. Por el motivo mencionado, es que no es necesario involucrar a terceros en la transacción.

La Biometría

Para poder identificar de forma unívoca a los usuarios de las diferentes plataformas asociadas al sistema blockchain de consorcio, es necesario apoyarse en la Biometría.

El reconocimiento biométrico se refiere al uso de diferentes características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como habla, firma o teclear). Estas características

se denominan identificadores biométricos o rasgos biométricos y sirven para reconocer automáticamente a los individuos. (Serratosa, 2012, p. 14)

Uno de los problemas principales que tienen las empresas desarrolladoras de videojuegos online o los operadores del juego, es que cuando los usuarios son registrados en su plataforma, solamente se les solicita un e-mail y algunos datos que pueden ser falsificados o reutilizados. Por ejemplo, una persona puede registrarse con diferentes cuentas de correo electrónico, diferentes ID de usuario y direcciones con nombres falsos. Al completar el registro, las personas deben confirmar el mail ingresado, para poder comenzar a utilizar el software o videojuego. Supongamos que el usuario decide utilizar programas externos para poder vencer de forma ilegítima a otros usuarios online, pero el sistema antitrampas que corre en el cliente detecta al usuario infringiendo las normas, por lo tanto al usuario se le prohíbe el acceso a la plataforma en la brevedad. El usuario no demora mucho tiempo en volver a la plataforma, utilizando otro email, un nuevo ID o nombre de usuario, y cualquier dirección falsa. Por el motivo mencionado es que todas las plataformas de videojuegos online deberían optar por un método de identificación unívoco para poder tomar decisiones en el futuro, adoptando alguno de los estándares de reconocimiento biométrico, ya sea el rostro, el iris o el que se prefiera. En la propuesta de intervención que mencionaremos a continuación, se optará por utilizar el reconocimiento facial como una alternativa posible, junto a una solución integral para estos inconvenientes.

Propuesta de Intervención

El sistema de penalización propuesto en este trabajo expone diferentes ventajas frente a los métodos tradicionales de castigo, el hecho de que un usuario sea identificado de forma unívoca permite tomar decisiones más sólidas con respecto a qué hacer con el usuario. Extender el registro a la toma de datos biométricos y no solamente a datos falsificables, habilita a las organizaciones a poder detener a las personas que busquen hacer trampas en los videojuegos de forma permanente y no solamente castigar a un ID de usuario. Además, la implementación de un sistema blockchain de consorcio, provocará que las empresas asociadas puedan reportar a los usuarios de sus plataformas y automáticamente los demás nodos o empresas, puedan tomar decisiones en cascada.

La propuesta no busca reemplazar en ningún momento a los sistemas antitrampas actuales, ya que en primer lugar estos deberán ser los responsables de detectar a los usuarios infractores. La plataforma servirá para tener un registro de la reputación de cada uno de los usuarios. No es de importancia si el sistema antitrampas utilizado se ejecuta en el cliente o en el servidor, si se trata del análisis de los datos estadísticos o si se detecta al usuario ejecutando un programa externo, o modificando la memoria RAM o la red. En cuanto el usuario sea detectado, la empresa podrá generar una transacción en el sistema blockchain, la cual será validada por los diferentes nodos y asentada sin poder ser manipulada. Los demás nodos pertenecientes al consorcio, podrán consultar los registros del sistema blockchain y en base a ello tomar una decisión en la base de datos de los usuarios local. Es importante destacar que la decisión final de prohibir el acceso del usuario, se delega a cada organización asociada al sistema, en este caso particular nos referimos a las empresas desarrolladoras u operadores del videojuego.

Para poder lograr lo mencionado anteriormente, lo primero que debe efectuarse es un acuerdo entre empresas u organizaciones que busquen frenar el avance de los usuarios tramposos, con el fin de asociarse y reportar información en el blockchain. Es importante destacar, que estas empresas deberán compartir intereses en común con respecto a las decisiones a tomar con estos individuos, el hecho de no reportar usuarios tramposos por la mayoría de los nodos o de reportar incorrectamente, podría incurrir en la corrupción del consorcio y acabaría en un sistema sin utilidad. Luego será necesario determinar un estándar de reconocimiento biométrico para establecer un protocolo de emisión de reportes. Cada empresa es responsable de la toma de los datos, almacenamiento y de la implementación para lograr esta recolección. En este trabajo se recomienda el reconocimiento facial, tomando la cámara del celular o de la computadora. La toma de información biométrica para los usuarios nuevos, se deberá realizar en el registro, mientras que la toma para los usuarios existentes, por única vez en cuanto el usuario acceda a la plataforma. Estos datos se deberán vincular al ID del usuario.

El esfuerzo del desarrollo para la implementación de la toma de datos, deberá correr por cuenta de cada una de las empresas asociadas al consorcio. Es importante destacar que el usuario puede negarse a la solicitud de la información, en tal caso, se deberá prohibir el acceso al ámbito multijugador online, posibilitando solamente al uso del software de forma local. De esta forma los demás usuarios podrán tener una mejor experiencia de juego sin la presencia de los usuarios problemáticos, y se evitarán las pérdidas económicas generadas por el retiro de los usuarios de la plataforma involucrada.

Con respecto al sistema blockchain, cualquier empresa o grupo de ellas que desee iniciar este proyecto, podría utilizar el Framework Hyperledger Fabric, para establecer un consorcio de empresas en el que se pueda registrar transacciones de la forma:

- Hash de los datos biométricos del usuario [*sha256*]
- Timestamp (Fecha y Hora de la transacción) [*date*]
- Reason (Motivo del reporte) [*string*]
- Report_Number (Número de reporte) [*int*]
- Source (Fuente u organización que reporta) [*int*]
- Overall_Status (Estado general) [*string*]

Es importante destacar que se menciona a la función criptográfica sha256, pero podría ser cualquier otro del grupo SHA-2, dependiendo de los estándares de seguridad a implementar. Con respecto al framework utilizado, no necesariamente debe tratarse de Hyperledger Fabric. En esta propuesta en particular, mencionamos a este framework por el grado de madurez alcanzado, en materia de generación de blockchains de consorcio.

Hyperledger Fabric es una plataforma de libro mayor distribuído, de nivel empresarial que ofrece modularidad y versatilidad para un abanico de casos de usos de la industria. La arquitectura modular se adapta a la diversidad de los casos de usos empresariales, a través de componentes del tipo plug-and-play, como consenso, privacidad y servicios de membresía. (Hyperledger Foundation, s.f). A diferencia de otros sistemas blockchains públicos que permiten participar a identidades desconocidas, en Hyperledger Fabric se utiliza un Proveedor de Servicio de Membresía mejor conocido como MSP o Membership Service Provider.Los diferentes nodos autorizados podrán unirse e intercambiar información acerca del estado de los usuarios.

Es importante destacar que para poder almacenar los datos biométricos de los usuarios, se deberá realizar la correspondiente disociación de la información. De ninguna manera se debe almacenar datos de los usuarios en un formato plano e interpretable por cualquiera, sino que deben estar encriptados bajo un algoritmo criptográfico confiable. Se debe tener en cuenta que cada país tiene sus regulaciones en cuanto a la ética y privacidad de los datos. En Europa, por ejemplo, a través del Reglamento general de protección de datos (RGPD), los usuarios pueden solicitar el borrado de sus datos personales de cualquier base de datos (Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo, 2016).

Conclusiones

La propuesta de intervención en el campo profesional en la que se está trabajando, busca complementar a los sistemas antitrampas actuales disuadiendo a los usuarios a que no realicen trampas en los videojuegos online, ya que de hacerlo, quedarían expuestos y podrían ser penalizados en todas las plataformas adheridas al sistema blockchain de consorcio. Esto traerá ciertos beneficios como por ejemplo, la continuidad del producto software y la permanencia de los usuarios en las plataformas.

Además evitará las pérdidas económicas generadas por la necesidad de actualizar continuamente los sistemas antitrampas, y por la disminución de la base de datos de usuarios activos del videojuego online. Por otro lado, constituirá un espacio colaborativo entre empresas que busquen frenar el avance de estos usuarios, mediante el compartimiento de la información de los usuarios conflictivos.

Los nodos que formen parte de este consorcio deberán estar alineados con respecto a la detención de estos usuarios infractores. De nada sirve generar un sistema blockchain, en el que el mayor número de los nodos se encuentren corruptos o no reporten la información correcta. Por otro lado, si bien la información con la que cuenten los stakeholders será de utilidad para la toma de decisiones, el derecho de admisión se le delega a cada uno de ellos para definir si los usuarios pueden hacer uso o no de su plataforma. De la misma forma, lo mencionado aplica para aquellos usuarios que no deseen brindar los datos biométricos para utilizar la plataforma.

Los conceptos abordados en este paper serán revisados en profundidad en el documento original de la propuesta de intervención en el campo profesional. En el mismo también se incluirá un plan para poder llevar adelante la implementación.

Referencias

Consalvo, M. (2007). *Cheating Gaining Advantage in Video Games*

[Las Trampas, obteniendo ventajas en Video Juegos]

Duh, H. B.-L. y Chen, V. H. H. (2009). *Cheating behaviors in online gaming*

[El comportamiento de los tramposos en juegos en línea]

Epic Games. (2023). *Don't bear with the cheaters*. [No tolere los tramposos]

Recuperado el 20 de junio de 2023 de https://www.easy.ac/en-us/#about

Hyperledger Foundation. (s.f). *Hyperledger Fabric: Open, Proven, Enterprise-grade DLT*.

[Hyperledger Fabric: Libro Mayor Abierto y Probado de Grado Empresarial]

Lehtonen, S. (2020). *Comparative Study of Anti-cheat Methods in Video Games*

[Estudio Comparativo de Métodos Antitrampas en videojuegos]

Mohanta, B., Panda, S. y Jena D. (2018). *An Overview of Smart Contract and Use cases in Blockchain Technology*. [Una descripción general de los Contratos Inteligentes y los Casos de uso en la tecnología Blockchain]

Postel, J. (28 de agosto de 1980). RF 768 *User Diagram Protocol.* IETF Datatracker.

Recuperado el 27 de agosto de 2023 de https://datatracker.ietf.org/doc/html/rfc768

Postel, J. (septiembre de 1981). RF 793 *Transmission Control Protocol.* IETF Datatracker.

Recuperado el 27 de agosto de 2023 de https://datatracker.ietf.org/doc/html/rfc793

Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas fisicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, L65 y L66, de 27 de abril de 2016.

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Riot Games (2020). *What is Vanguard?* [¿Qué es el Vanguard?]

https://support-valorant.riotgames.com/hc/en-us/articles/360046160933-What-is-Vanguard-

Serratosa, F (2012). La biometría para la identificación de las personas

Valve Corporation. (s.f). *What is VAC?* [¿Qué es el VAC?]
https://help.steampowered.com/en/faqs/view/571A-97DA-70E9-FF74

Van de Ven, B. (2023). *Cheating and anti-cheat system action impacts on user experience*
[Las trampas y la acción de los sistemas antitrampas impactan en la experiencia del usuario]

Zheng, Z., Xie, S., Dai, H., Chen, X. y Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. [Un Resumen de la Tecnología Blockchain: Arquitectura, Consenso y Futuras Tendencias]