**TECNOLOGÍAS DE REGISTROS DISTRIBUIDOS (DLT)**

Es un sistema digital que nació de la red peer-to-peer (P2P) que permiten registrar información en múltiples ubicaciones en un momento dado. DLT, a diferencia de las bases de datos tradicionales, no tiene un lugar central para almacenar información y esta función de descentralización también proporciona mayor seguridad, transparencia y confianza entre las partes que la utilizan. Y una de las tendencias de usos de los DLT son las aplicaciones descentralizadas o DApps

**DAG.-** por su traducción, grafos acíclicos dirigidos, esta tecnología no utiliza la cadenas de bloques como blockchain y tampoco utiliza mineros que son computadoras físicas de altas gamas para concatenar transacciones sino que utiliza grafos y dispositivos clientes como celulares computadoras para concatenar las transacciones, lo que lo hace rápida y barata porque no se pagan comisiones de aquí se origina el termino Tangle y la tecnología IOTA es fruto de esto.

**BLOCKCHAIN.-**  utiliza la cadena de bloques y aquí si existen mineros lo que lo hace menos eficiente en términos de velocidad de concatenación y comisiones que los DAG.

**TEMPO.-** es un DLT relativamente nuevo y es una mejora del blockchain en el aspecto de que no utiliza protocolos de consenso para concatenar transacciones sino que se basa en una marca de tiempo.

**IOTA.-** pertenece al DLT de tipo Tangle, es pública y su principal característica es que no utiliza mineros por lo que registrar transacciones en su red es totalmente gratuita sin pagar comisión

**IOTEX.-** es un hibrido y es pública es una mezcla entre un Tangle y blockchain y gracias a que es un hibrido las comisiones que cobran para por ejemplo para deployar un smart contract son muy bajas a comparación con otras blockchain.

**TATUM.-** es una plataforma blockchain de tipo consorcio debido a que ofrece distintas Apis para conectarse con multiples tecnologías blockchain y tienen redes blockchain gratuitas y de paga.

**Almacenamiento seguro**

El almacenamiento seguro es importante destacarlo debido a que en esta investigación trató sobre transacciones financieras en aplicaciones Fintech y estas deben brindar seguridad de los datos tanto en el transporte como en el almacenamiento de la información, para esto se tomó a consideración el mapa conceptual elaborado por los autores Kumar y Goyal donde indican cuatro categorías a tener en cuenta en la seguridad de la cloud computing que es otro aspecto que también se utilizó en esta investigación cuyas arquitecturas y microservicios fueron implementados bajo la plataforma de Google Cloud. Y todos estos aspectos que se ven ahora en la diapositiva fueron tomados en cuenta para ser implementadas tantos en las arquitecturas como en los microservicios.

**Aplicaciones Fintech**

Las Fintech se refieren a todas aquellas empresas que utilizan la tecnología para mejorar o automatizar sus procesos o servicios financieros brindando funcionalidades como por ejemplo integración con blockchain, billeteras virtuales, pagos online entre otros.

**Total de ganancias mensuales**

El dinero perdido fue menor con respecto al dinero obtenido por disputadas ganadas siendo el total de ganancias por disputas ganadas de $2.566,39 a comparación con los $559,36 perdidos.

**Encuestas de Estafas**

El total de encuestados fueron 85 usuarios seleccionados a partir de las 255 transacciones que se tomaron como muestra.

**Usuarios con identidad digital Y NFT**

Alto interés de usuarios por tener cuentas verificadas con sus propias identidades digitales dentro del mundo de la blockchain.

**Comprobación de hipótesis**

Debido a que el valor obtenido en SPSS fue de 0.89 y según el autor Akoglu, si el valor obtenido es mayor a 0.7 se concluye que existe una correlación positiva significativa o fuerte. Por lo tanto, se comprueba la hipótesis planteada en la investigación.

**Probabilidad de ganar disputas financieras por fraudes**

De las 255 transacciones tomadas como muestra, se incluyeron tantos pagos detectados como potencialmente estafas y fraudulentas entre los meses de enero, febrero, marzo y abril del año 2022, de las cuales 138 de esas transacciones fueron fraudes.

**Seguridad contra ataques man-in-the- middle.**

Aplicación de encriptación RSA con tamaño de 4096 bits en llaves públicas y privadas de criptomonedas y almacenamiento en la base de datos criptográfica de IOTA Stronghold para protección de la información.

**Identidad digital con NFT.**

Obtención de una identidad digital dentro del blockchain a través de verificación biométrica de usuarios y NFT, aumentando las probabilidades de reducir casos de fraudes en pagos con tarjetas.

**Transacciones de criptomonedas con comisiones bajas o cero.**

Comisión baja gracias a IoTex Blockchain durante pagos y comisiones con valor cero con IOTA que gracias a su inmutabilidad sirvieron de apoyo durante el dispute de fraudes de primera persona con las entidades bancarias.