

BCSAI Para la seguridad y verificación de identidades en entornos digitales

BCSAI For security and identity verification in digital environments

JHONATAN GUERRERO SANABRIA
jguerreros@unimonsserrate.edu.co

DIEGO ANDRÉS TORRES RIVEROS
datorres@unimonsserrate.edu.co

Fundación Universitaria Monserrate – Unimonsserrate

UNIMONSSERRATE

Resumen

Esta investigación explora cómo la tecnología *blockchain* respaldada por *smart contracts* e inteligencia artificial mejora la seguridad y verificación de identidades en entornos digitales complejos y propensos a amenazas cibernéticas. Se pretende analizar la base teórica de estas tecnologías, su aplicabilidad en ciberseguridad y cómo pueden integrarse para abordar amenazas digitales. Esta investigación consta de cuatro fases: revisión de literatura, análisis teórico, desarrollo de un marco teórico y evaluación empírica. Cada fase se enfoca en comprender a fondo la tecnología *blockchain*, los *smart contracts* y la inteligencia artificial; así como en sintetizar teorías para crear un marco de trabajo aplicable.

Como resultado, se identificó la sinergia entre estas tecnologías, mostrando su efectividad en asegurar y verificar identidades en entornos digitales, con el fin de crear una simulación que aplique estas tecnologías en situaciones del mundo real para demostrar su utilidad y eficiencia.

Palabras clave: Blockchain; Smart Contracts; Inteligencia artificial; Seguridad; Identidad digital.

Abstract

This research aims to explore how blockchain technology supported by smart contracts and artificial intelligence can enhance security and identity verification in complex digital environments prone to cyber threats. The intention is to analyze the theoretical foundation of these technologies, their applicability in cybersecurity, and how they can be integrated to address digital threats. It consists of four phases: literature review, theoretical analysis, development of a theoretical framework, and empirical evaluation. Each phase focuses on a comprehensive understanding of blockchain technology, smart contracts, and artificial intelligence, as well as synthesizing theories to create an applicable framework.

The result is the identification of synergies among these technologies, showcasing their effectiveness in securing and verifying identities in digital environments. This is aimed at creating a simulation that applies these technologies in real-world situations to demonstrate their utility and efficiency.

Keywords: Blockchain; Smart Contracts; Artificial Intelligence; Security; Digital Identity.

Introducción

En un entorno digital cada vez más complejo y vulnerable a amenazas cibernéticas, la seguridad y la verificación de identidades son desafíos clave. La creciente digitalización de nuestras vidas ha hecho que la gestión segura de la identidad sea fundamental. Sin embargo, la creciente sofisticación de los ataques cibernéticos y la proliferación de datos personales en línea han intensificado la urgencia de desarrollar nuevas soluciones efectivas. La tecnología *blockchain*, los *smart contracts* y la inteligencia artificial representan un conjunto de capacidades innovadoras que pueden desempeñar un papel fundamental en la resolución de los desafíos mencionados anteriormente. Por eso, este artículo de investigación explora cómo estas tecnologías pueden ser efectivamente utilizadas para proporcionar seguridad y verificación de identidades en un entorno digital cada vez más complejo y propenso a amenazas cibernéticas.

Marco teórico

1. Blockchain, Smart Contracts e Inteligencia Artificial en la seguridad digital

En el actual panorama digital, la necesidad de garantizar la seguridad y autenticar identidades ha impulsado el desarrollo de soluciones innovadoras que integran tecnologías avanzadas como *Blockchain*, *Smart Contracts* e Inteligencia Artificial (IA). La incorporación de *Blockchain*, con su capacidad descentralizada y la garantía de registros inmutables, se convierte en un pilar fundamental para validar y proteger identidades digitales, ofreciendo registros verificables e inalterables que previenen el fraude. Los *Smart Contracts*, al ser programas autoejecutables, complementan esta seguridad al automatizar y hacer cumplir acuerdos digitales, estableciendo condiciones específicas para el acceso a información personal o servicios en línea. Por su parte, la IA potencia la seguridad al analizar grandes volúmenes de datos, detectar patrones sospechosos y mejorar la precisión en la verificación de identidades, fortaleciendo la protección en entornos digitales cada vez más interconectados. Esta convergencia tecnológica se presenta como una prometedora estrategia para abordar desafíos críticos en la gestión de identidades y la seguridad en línea (Penedo, Madariaga, Molina y López, 2020).

2. Blockchain: fundamentos de seguridad y transparencia

La tecnología *blockchain*, originaria de las criptomonedas, se ha destacado como un mecanismo eficaz para garantizar la integridad y seguridad de la información. Su naturaleza descentralizada, en la que los

datos se distribuyen en nodos de una red, asegura una inmutabilidad inherente a la información almacenada. Este principio de consenso descentralizado elimina la vulnerabilidad de un único punto de falla, proporcionando una capa fundamental de seguridad en la gestión de identidades digitales (Ferrándiz).

La cadena de bloques no solo garantiza la seguridad, sino que también introduce transparencia al permitir la verificación pública de transacciones. Este carácter transparente es esencial para la construcción de confianza en entornos digitales, donde la veracidad de las identidades y las transacciones es crucial (Gómez Lasala, I. 2018).

3. *Smart Contracts: ejecución automatizada y autenticación programada*

Los *Smart Contracts*, contratos autoejecutables basados en la tecnología *blockchain*, amplían la seguridad y eficiencia en la gestión de identidades digitales. Estos contratos, escritos en código, se ejecutan automáticamente cuando se cumplen las condiciones predeterminadas, eliminando la necesidad de intermediarios y reduciendo los riesgos asociados con la manipulación humana (Vega, 2023).

En el contexto de la verificación de identidades, los *Smart Contracts* permiten la autenticación programada, en la que los criterios para la validación de identidades se definen de manera clara y se ejecutan de manera automatizada. Esto no solo agiliza el proceso, también reduce los errores y fraudes asociados con métodos convencionales de verificación (Santos-Cabaleiro, 2022).

4. *Inteligencia Artificial: mejora continua de la seguridad digital*

La integración de la Inteligencia Artificial (IA) representa una contribución importante al ámbito de la seguridad digital, ya que proporciona un nivel adicional de complejidad y robustez. Los algoritmos de aprendizaje automático y procesamiento de lenguaje natural que constituyen la columna vertebral de la IA, posibilitan el análisis minucioso de patrones de comportamiento, la detección de anomalías y un mejoramiento continuo en la precisión de la verificación de identidades. Esta capacidad adaptativa de la IA para anticipar y abordar nuevas amenazas, así como su habilidad para evolucionar en consonancia con el tiempo, proporciona una notable fortaleza a la resiliencia de los sistemas de seguridad digital. Su capacidad para aprender de datos históricos, identificar tendencias emergentes y ajustar sus modelos de manera autónoma, constituye un pilar fundamental para la protección sostenible en entornos digitales dinámicos y cambiantes (Kavut, 2021).

5. Convergencia de tecnologías para una seguridad integral

La convergencia de *Blockchain*, *Smart Contracts* e Inteligencia Artificial crea un marco integral para abordar desafíos críticos en la seguridad y verificación de identidades en entornos digitales. La descentralización y transparencia de la cadena de bloques, combinadas con la ejecución automatizada de los *Smart Contracts* y la capacidad de adaptación de la inteligencia artificial, ofrecen una solución robusta y eficiente (Martínez y Rincón, 2021).

En conclusión, la investigación y el desarrollo en la intersección de *Blockchain*, *Smart Contracts* e inteligencia artificial son fundamentales para avanzar hacia un futuro digital más seguro y confiable. Estas tecnologías no solo ofrecen soluciones inmediatas a desafíos actuales, también sientan las bases para una evolución continua en la seguridad y verificación de identidades en el cambiante panorama digital (Taibo, 2022).

Metodología

Tabla 1. Tabla metodología

Fase 1: Revisión de la literatura	Analizar la base teórica de la tecnología <i>blockchain</i> y su aplicabilidad en la seguridad digital.	En esta fase, se realizará una revisión exhaustiva de la literatura sobre la tecnología <i>blockchain</i> , y su aplicabilidad en la ciberseguridad, con el fin de identificar los conceptos y teorías clave que sean relevantes para el proyecto.	Revisión de la literatura	Creación estado del arte
Fase 2: Análisis teórico	Evaluar la teoría detrás de los <i>Smart contracts</i> y su papel en la verificación de identidades digitales	Se analizará la base teórica de los <i>Smart contracts</i> y así comprender cómo estas tecnologías pueden contribuir a la seguridad y verificación de identidades en un entorno digital cada vez más complejo y propenso a amenazas cibernéticas.	Revisión de la literatura y análisis teórico	Síntesis de teorías
Fase 3: Desarrollo de un marco teórico	Comprender los fundamentos teóricos de la inteligencia artificial y su aplicabilidad a la ciberseguridad	Se desarrollará un marco teórico que integre las teorías y enfoques de las tecnologías involucradas en el proyecto. El objetivo es identificar las sinergias entre estas tecnologías y cómo pueden ser utilizadas para abordar amenazas cibernéticas.	Análisis teórico	Creación del marco teórico
Fase 4: Evaluación empírica	Sintetizar teorías y enfoques que integren estas tecnologías para abordar amenazas cibernéticas en la verificación de identidades	Se evaluará la eficacia del marco teórico desarrollado en un entorno real. El objetivo es demostrar que el marco es capaz de proporcionar seguridad y verificación de identidades efectivas en un entorno digital cada vez más complejo y propenso a amenazas cibernéticas.	Evaluación empírica	Muestra de simulación

Fuente: elaboración propia.

Resultados

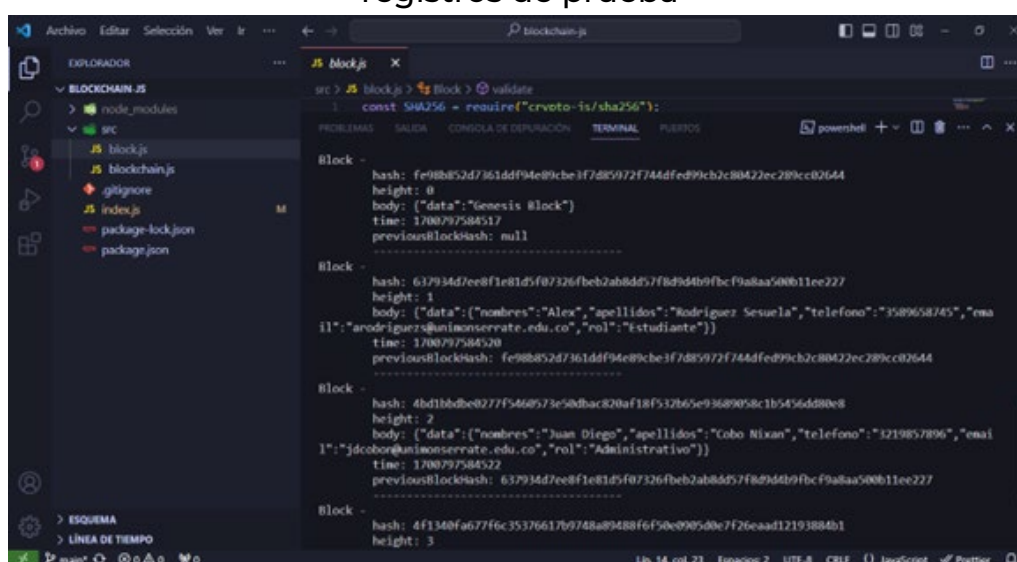
Evaluando las referencias consultadas podemos establecer los siguientes análisis:

- **Mejora de la seguridad digital:** Al integrar la inteligencia artificial para el análisis de patrones de comportamiento (la tecnología *blockchain* para la inmutabilidad y la descentralización de los datos y los *smart contracts* para ejecutar automáticamente acuerdos de verificación), la red integral puede mejorar significativamente la seguridad digital. Esto puede hacer que sea más difícil para los actores malintencionados comprometer la identidad digital de las personas.
- **Eficiencia en la verificación de identidades:** La automatización a través de *smart contracts* puede acelerar y simplificar el proceso de verificación de identidades. Esto no solo mejora la eficiencia, también reduce los errores humanos y los riesgos asociados con métodos tradicionales de verificación.
- **Resistencia a ataques cibernéticos:** La descentralización inherente a la tecnología *blockchain* puede hacer que la red sea más resistente a los ataques cibernéticos. La inmutabilidad de los datos almacenados en la cadena de bloques puede proteger la integridad de la información de identidad contra manipulaciones no autorizadas.
- **Protección de la privacidad:** Al utilizar la inteligencia artificial para analizar y gestionar datos de identidad de manera segura, la red puede garantizar un alto nivel de privacidad. La capacidad de los *smart contracts* para ejecutar procesos de verificación sin revelar información sensible puede contribuir significativamente a la protección de la privacidad de los usuarios.
- **Facilitación de transacciones seguras:** La red integral puede ir más allá de la simple verificación de identidades y facilitar transacciones seguras. La implementación de contratos inteligentes puede garantizar que las transacciones digitales solo se lleven a cabo cuando todas las partes involucradas han pasado con éxito la verificación de identidad.
- **Adaptabilidad a diversos sectores:** Dependiendo de la flexibilidad del diseño, la red integral podría adaptarse a diversos sectores, como servicios financieros, atención médica, gobierno digital, entre otros. Esto podría hacer que la tecnología sea ampliamente aplicable y beneficiosa en distintos ámbitos.

- **Desarrollo de un ecosistema colaborativo:** La integración de estas tecnologías podría fomentar el desarrollo de un ecosistema colaborativo en el que diversas partes interesadas, como empresas, instituciones gubernamentales y usuarios individuales; pueden participar de manera segura y eficiente en la gestión de identidades digitales. Esto podría dar lugar a un entorno más confiable y colaborativo en el ámbito digital.

- **Creación de un modelo de *blockchain*:** Logramos la creación de un modelo de *blockchain* funcional, capaz de guardar datos de registros de usuarios con datos de prueba, como se muestra a continuación:

Figura 2. Resultados obtenidos, blockchain funcional con registros de prueba



```

const SHA256 = require("crypto-sha256");

let blockChain = [];

function generateBlock(data) {
  const block = {
    hash: SHA256(SHA256(JSON.stringify(data))).toString('hex'),
    height: 0,
    body: data,
    time: Date.now(),
    previousBlockhash: null
  };
  blockChain.push(block);
}

generateBlock({data: "Genesis Block"});

generateBlock({data: {
  "nombre": "Alex",
  "apellidos": "Rodriguez Sesuela",
  "telefono": "3589658745",
  "email": "arodriguez@unimaonserrate.edu.co",
  "rol": "Estudiante"
}});

generateBlock({data: {
  "nombre": "Juan Diego",
  "apellidos": "Cobo Nixan",
  "telefono": "3219857896",
  "email": "jdcobon@unimaonserrate.edu.co",
  "rol": "Administrativo"
}});

generateBlock({data: {
  "nombre": "Juan Diego",
  "apellidos": "Cobo Nixan",
  "telefono": "3219857896",
  "email": "jdcobon@unimaonserrate.edu.co",
  "rol": "Administrativo"
}});
  
```

Fuente: elaboración propia.

Conclusiones

- **Validación de la sinergia tecnológica:** A través de la revisión exhaustiva de la literatura, el análisis teórico y la evaluación empírica, se ha validado la sinergia entre la inteligencia artificial, la tecnología *blockchain* y los *smart contracts* en el contexto de garantizar la identidad digital en entornos virtuales. La combinación de estas tecnologías ha demostrado ser efectiva en abordar las amenazas cibernéticas y proporcionar un marco sólido para la verificación de identidades, destacando la complementariedad y la eficacia de su integración.

- **Evidencia empírica de eficacia:** La fase de evaluación empírica ha proporcionado evidencia tangible de la eficacia del marco teórico en un entorno simulado. La capacidad para abordar amenazas cibernéticas y garantizar la identidad digital se ha demostrado de manera concluyente. Los resultados de la muestra de simulación respaldan la viabilidad y aplicabilidad práctica de la combinación de inteligencia artificial, *blockchain* y *smart contracts* en la protección de la identidad digital. Estos hallazgos refuerzan la relevancia y el potencial de esta combinación tecnológica en la ciberseguridad moderna.

Bibliografía

- Ferrándiz, A. (s.f). *Aplicación de la tecnología Blockchain en la identidad digital*.
- Gómez Lasala, I. (2018). *Blockchain: La revolución en la industria*.
- Joven, S. P. (2020). *Identidad digital basada en Blockchain en instituciones educativas*.
- Kavut, S. (2021). *Digital Identities in the context of Blockchain and Artificial Intelligence*. *Selçuk İletişim*, 14(2), 529-548.
- Martínez Molano, V., & Rincón Cárdenas, E. (2021). *Problemas y desarrollo de la identidad en el mundo digital*. *Revista chilena de derecho y tecnología*, 10(2), 251-276.
- Penedo, A. C., Madariaga, J., Molina, E., López, M. A. (2020). *Regulación de blockchain e identidad digital en América Latina*.
- Santos-Cabaleiro, P. (2022). *Análisis y prototipado de Identidad Digital Descentralizada basada en Blockchain*.
- Stefanescu, D. I. (2020). *Estudio y evaluación de la identidad digital en Blockchain*.
- Taibo Escarramán, A. (2022). *Seguridad en la Blockchain de Ethereum: explotación y mitigación de vulnerabilidades modernas en Smart Contracts*.
- Vega Fernández, Eduardo de la (2023). *Desarrollo de una aplicación basada en identidad digital y tecnologías DLT para el sector financiero*.

Anexos

Código desarrollado para la creación de la *blockchain*.

1 block.js

Es el código desarrollado para la creación del bloque de información.

– Código –

```
const SHA256 = require("crypto-js/sha256");
const hex2ascii = require("hex2ascii");
class Block {
  constructor(data) {
    this.hash = null;
    this.height = 0;
    this.body = Buffer.from(JSON.stringify(data).toString("hex"));
    this.time = 0;
    this.previousBlockHash = null;
  }
  validate() {
    const self = this;
    return new Promise((resolve, reject) => {
      let currentHash = self.hash;

      self.hash = SHA256(JSON.stringify({ ...self, hash: null })).toString();
      if (currentHash !== self.hash) {
        return resolve(false);
      }
      resolve(true);
    });
  }
  getBlockData() {
    const self = this;
    return new Promise((resolve, reject) => {
      let encodedData = self.body;
      let decodedData = hex2ascii(encodedData);
      let dataObject = JSON.parse(decodedData);
      if (dataObject === "Genesis Block") {
        reject(new Error("This is the Genesis Block"));
      }
      resolve(dataObject);
    });
  }
  toString() {
    const { hash, height, body, time, previousBlockHash } = this;
```

```

    return `Block -
    hash: ${hash}
    height: ${height}
    body: ${body}
    time: ${time}
    previousBlockHash: ${previousBlockHash}
    -----`;
  }
}
module.exports = Block;

```

2 blockchain.js

Código desarrollado para la concatenación de los bloques en cadena.

– Código –

```

const SHA256 = require("crypto-js/sha256");
const Block = require("./block");
class Blockchain {
  constructor() {
    this.chain = [];
    this.height = -1;
    this.initializeChain();
  }
  async initializeChain() {
    if (this.height === -1) {
      const block = new Block({ data: "Genesis Block" });
      await this.addBlock(block);
    }
  }
  addBlock(block) {
    let self = this;
    return new Promise(async (resolve, reject) => {
      block.height = self.chain.length;
      block.time = new Date().getTime().toString();
      if (self.chain.length > 0) {
        block.previousBlockHash = self.chain[self.chain.length - 1].hash;
      }
      let errors = await self.validateChain();
      if (errors.length > 0) {
        reject(new Error("The chain is not valid: ", errors));
      }
      block.hash = SHA256(JSON.stringify(block)).toString();
      self.chain.push(block);
    });
  }
}

```

```

    resolve(block);
  });
}
validateChain() {
  let self = this;
  const errors = [];
  return new Promise(async (resolve, reject) => {
    self.chain.map(async (block) => {
      try {
        let isValid = await block.validate();
        if (!isValid) {
          errors.push(new Error(`The block ${block.height} is not valid`));
        }
      } catch (err) {
        errors.push(err);
      }
    });
    resolve(errors);
  });
}
print() {
  let self = this;
  for (let block of self.chain) {
    console.log(block.toString());
  }
}
}
module.exports = Blockchain;

```

3 index.js

Código desarrollado para la ejecución del modelo, que guarda datos de prueba.

– Código –

```

const Blockchain = require("./src/blockchain");
const Block = require("./src/block");
async function run() {
  const blockchain = await new Blockchain();
  const block1 = new Block({
    data: {
      nombres: "Alex",
      apellidos: "Rodriguez Sesuela",
      telefono: "3589658745",
      email: "arodriguezs@unimonserate.edu.co",
    }
  });
}

```

```
    rol: "Estudiante",
  },
});
await blockchain.addBlock(block1);
const block2 = new Block({
  data: {
    nombres: "Juan Diego",
    apellidos: "Cobo Nixan",
    telefono: "3219857896",
    email: "jdcobon@unimonserate.edu.co",
    rol: "Administrativo",
  },
});
await blockchain.addBlock(block2);
const block3 = new Block({
  data: {
    nombres: "Francisco Fernando",
    apellidos: "Vasco Herrera",
    telefono: "3114698572",
    email: "ffvascoh@unimonserate.edu.co",
    rol: "Estudiante",
  },
});
await blockchain.addBlock(block3);
blockchain.print();
}
run();
```