

TODO SOBRE BLOCKCHAIN Y SU ROL EN LA CIBERSEGURIDAD APUNTES ESENCIALES



Vista previa del documento.

Mostrando 6 páginas de 36

Indice



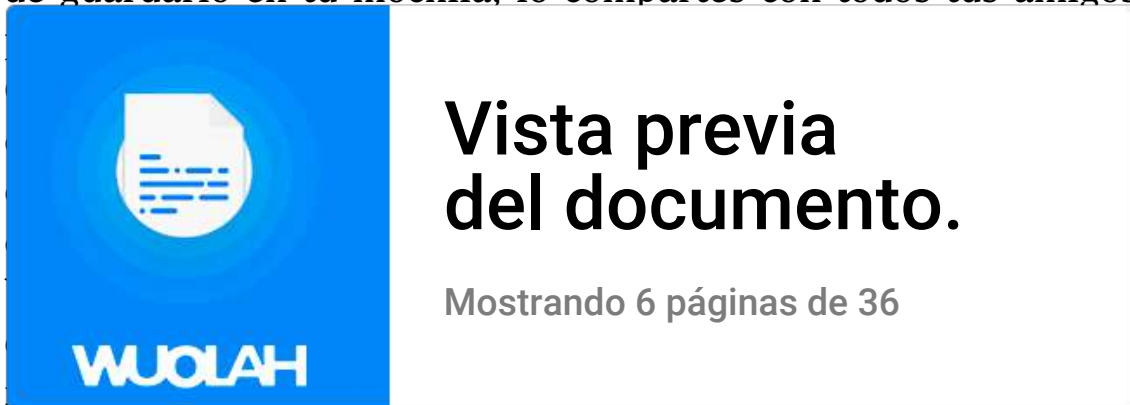
Vista previa del documento.

Mostrando 6 páginas de 36

1. ¿Qué es Blockchain?

1.1 Definición y conceptos básicos

Blockchain es una tecnología que funciona como un libro de registros digital, pero con un giro especial: no lo guarda una sola persona o empresa, sino que muchas computadoras lo tienen al mismo tiempo. Imagina un cuaderno donde apuntas todo lo que pasa (como quién te debe dinero o qué compraste), pero en lugar de guardarlo en tu mochila, lo compartes con todos tus amigos

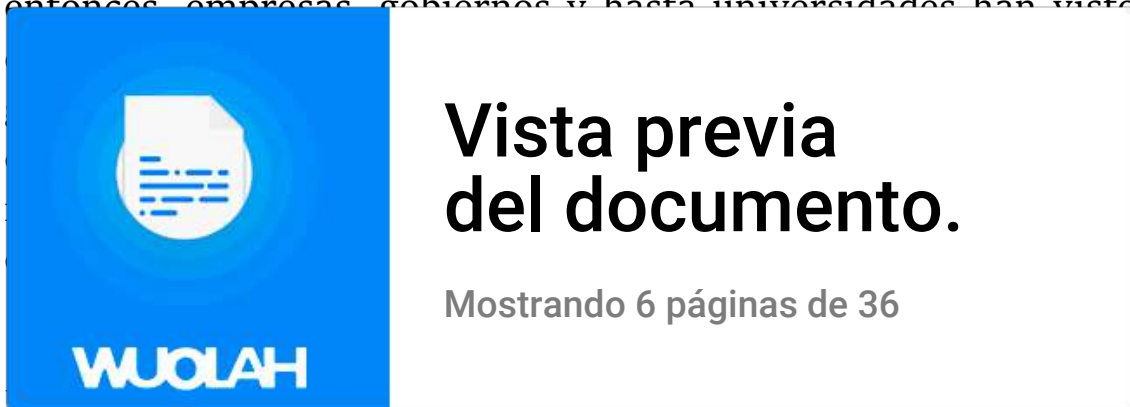


criptomonedas o seguridad digital. Para estudiantes, piensen en esto como una forma de asegurarse de que nadie haga trampa en un juego o proyecto grupal porque todos tienen la misma copia de las reglas.

Ejemplo simple: Imagina que en clase anotamos quién prestó un lápiz a quién en un cuaderno compartido. Si Juan escribe "María me debe un lápiz" y todos lo copian, María no puede borrar eso sin que todos lo notemos.

1.2 Historia y origen

La idea de blockchain empezó en 2008, cuando alguien (o un grupo) usando el nombre Satoshi Nakamoto escribió un artículo explicando cómo crear dinero digital sin bancos, llamado Bitcoin. Nadie sabe quién es Satoshi, pero su idea cambió el mundo. En 2009, se puso en marcha la primera blockchain para hacer funcionar Bitcoin, permitiendo que la gente enviara dinero por internet sin que un banco dijera "sí" o "no". Al principio, todos pensaban que blockchain solo servía para criptomonedas, pero luego, en 2015, apareció Ethereum, que añadió "contratos inteligentes" (reglas automáticas dentro de la cadena). Desde entonces, empresas, gobiernos y hasta universidades han visto



Ejemplo de un juego que en 2009 alguien dijo: "¡Oye, vamos a hacer un juego donde todos anotamos puntos sin un árbitro". Ese fue Bitcoin. Luego, alguien más dijo: "¡Oye, también podemos anotar quién ganó sin discutir!" Eso fue Ethereum.

1.3 Características principales

Blockchain tiene cosas que lo hacen especial y diferente de otros sistemas:

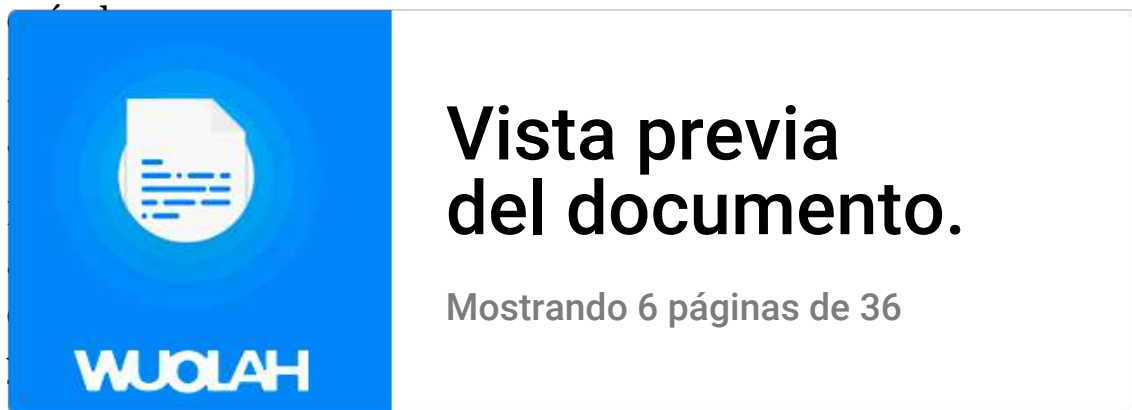
Inmutabilidad: Una vez que escribes algo, no lo puedes borrar ni cambiar sin permiso de todos. Es como escribir con tinta permanente en un cuaderno público.

Descentralización: No hay un jefe o servidor principal; muchas computadoras guardan la misma información. Si una falla, las demás siguen funcionando.

Transparencia: En las blockchains públicas, todos pueden ver qué se escribió (aunque a veces está protegido para que no se entienda sin permiso).

Seguridad: Usa códigos secretos y matemáticas para que nadie pueda meterse a cambiar cosas sin que lo notemos.

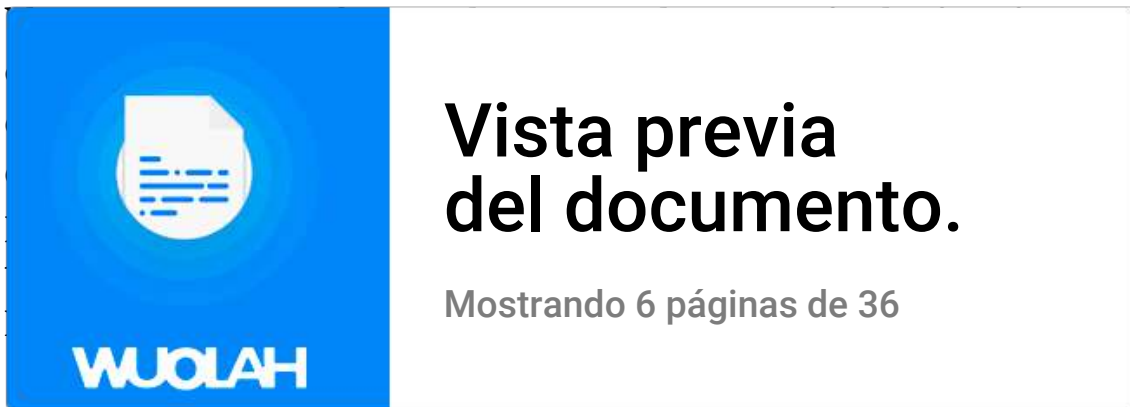
Trazabilidad: Puedes ver todo el historial, como quién hizo qué y



2. Cómo Funciona Blockchain

2.1 Estructura de bloques y cadenas

Blockchain organiza la información en pedacitos llamados "bloques". Cada bloque es como una página de un cuaderno que tiene tres partes principales: los datos (lo que quieres guardar, como "Pedro le dio 5 euros a Ana"), un hash (un código único como un número de identificación de esa página), y el hash del bloque anterior (que lo conecta con la página de antes). Estos



Ejemplo simple: Supón que escribimos: "Día 1: Ana trajo agua. Día 2: Pedro trajo galletas". Cada día es un bloque, y el Día 2 tiene un sello que dice "viene del Día 1". Si alguien borra el agua de Ana, el sello del Día 2 no encaja y sabemos que algo pasó.

2.2 Mecanismos de consenso

Como blockchain no tiene un jefe, las computadoras (nodos) deben ponerse de acuerdo sobre qué bloques añadir. Esto se hace con "mecanismos de consenso", que son como reglas de votación.