universidad de león

Ataques a Criptomonedas y seguimiento de carteras digitales

Alumno: Javier Rodríguez Villalobos
Tutor: Ricardo J. Rodríguez Fernández

Introducción - Hitos

- 1983 - David Chaum, fundamentos pagos electrónicos
- 1991 - Haber y Scott-Stornetta, definición blockchain (1991)
- 1992 - Timothy C. May, Movimiento CypherPunk
- 2008 - Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*
- 2009 - Creación del bloque 1 de la cadena bitcoin
- 17/12/17 - Precio máximo del Bitcoin 19,798.68 USD

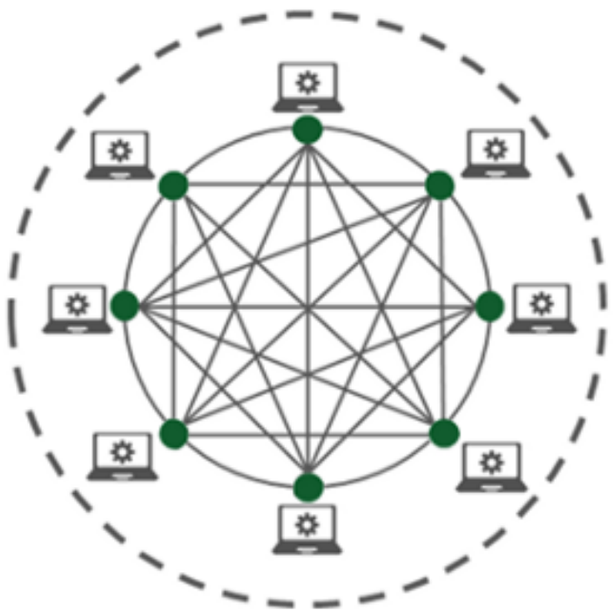
¿Qué es el blockchain?

- Sistema de registro distribuido
- Conjuntos de datos validados por operaciones criptográficas
- Información enlazada entre sí
- Características:
  - Descentralización
  - Transparencia
  - Confiabilidad
  - Inmutabilidad
  - Privacidad

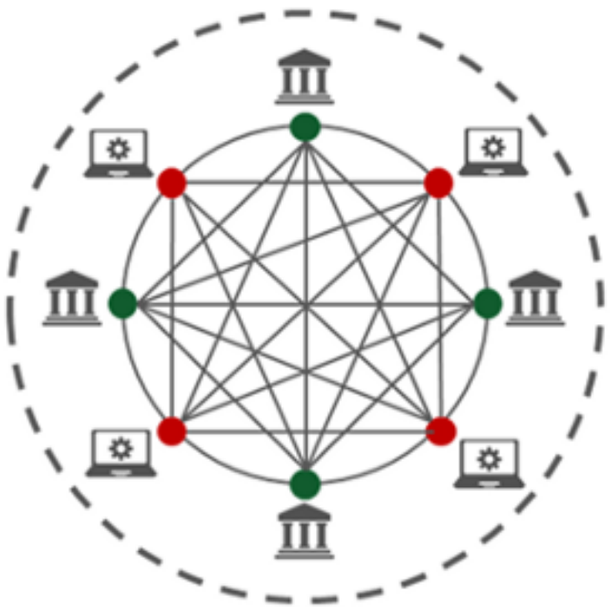
Desventajas de la tecnología

- Inmutabilidad de la información
- Ausencia de marco regulatorio y legal
- Velocidad del procesamiento de la información
- Excesiva cantidad de recursos utilizados
- Relación con actividades ilegales
- Escalabilidad del sistema
- La existencia de bugs y vulnerabilidades
- Costes más altos respecto a otras tecnologías

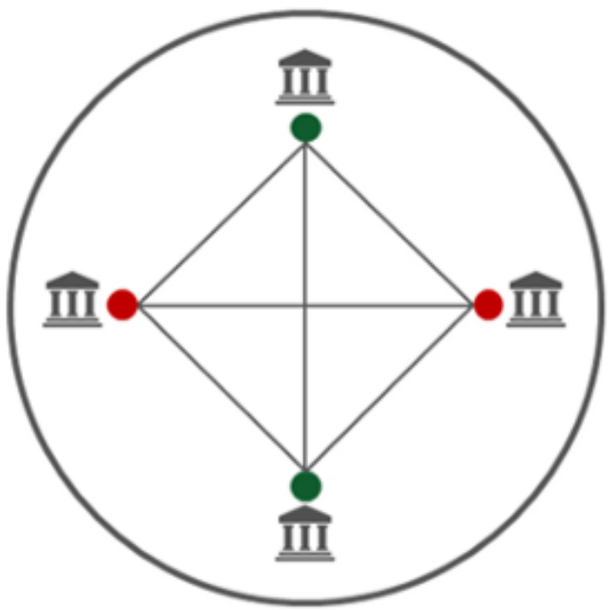
Tipos de redes Blockchain



Pública



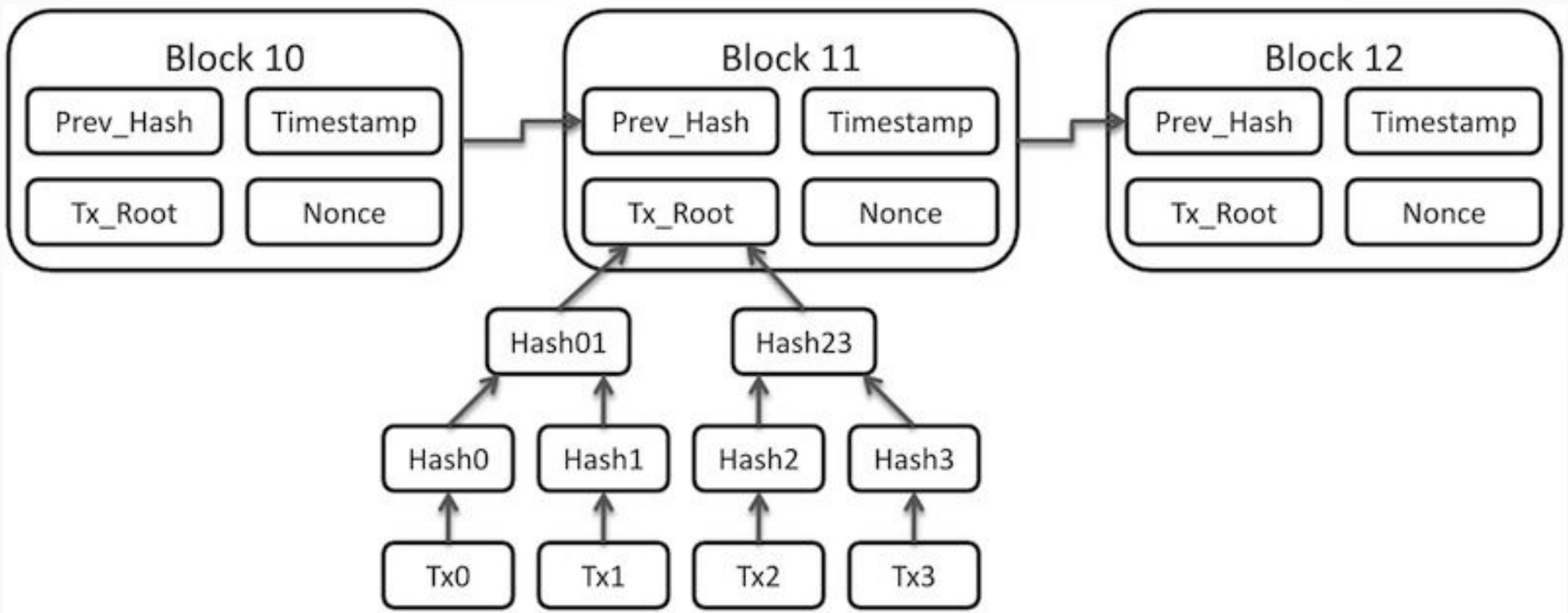
Híbrida



Privada

Funcionamiento del blockchain

Partes del bloque



Mecanismos de consenso I

Mecanismo de consenso	Principales ventajas	Principales desventajas
PBFT	Eficiencia energética al no necesitarse a otro para la validación	Centralización en uno o pocos nodos. Vulnerable a ataques Sybil
PoW	Cálculo de hashes potentes y seguros	Gasto de energía y poder computacional elevado. Vulnerable a ataques del 51%
PoA	Escalabilidad, eficiencia computacional y rapidez de validación	Censura. Vulnerable frente a ataques DDOS o Sybil.
PoET	Coste de participación en la validación es muy bajo	Inoperable en blockchains públicas
PoC	Eficiencia computacional	Vulnerable al malware
PoB	Gasto energético y en equipamiento bastante menor.	Gasto operacional elevado y es vulnerable al ataque del 51%.
PoS	Gasto energético menor. Prima la participación de los nodos	Concentración de la validación en pocos nodos. Vulnerable a los ataques DDOS y Eclipse

Mecanismos de consenso II

Nombre	Mecanismo de consenso	Nombre	Mecanismo de consenso
Bitcoin	PoW	Cardano	PoS
Ethereum	PoS	IOTA	PBFT
Ripple	PBFT	NEO	PBFT
Bitcoin Cash	PoW	Monero	PoW
Litecoin	PoW	Dash	PoW-PoS
Stellar	PBFT	Zcash	PoS

Qué es la pseudoanonimización

Capa de privacidad para que no se identifiquen a las partes intervinientes en la operación

TIPOS

- Enlazable: Se puede consultar las carteras, el importe y la fecha
- No enlazable: Se evita incluir los datos relativos a las carteras

Características criptomonedas

Nombre	Lenguaje de programación	Algoritmo de encriptación	Pseudo-anonimización
Bitcoin	C++	SHA-256d	Enlazable
Ethereum	C++, Go, Rust	Etash	Enlazable
Ripple	C++	ECDSA	Enlazable
Bitcoin Cash	C++	SHA-256d	Enlazable
Litecoin	C++	SHA-256d	Enlazable
Stellar	C++, Go, Java	FBA	Enlazable
IOTA	Java	SHA-3	Enlazable
NEO	C#	SHA256 y RIPEMD160	Enlazable
Zcash	C++	EquiHash	Inenlazable
Monero	C++	CryptoNight	Inenlazable
Dash	C++	X11	Inenlazable

Formas de desanonimización

- Formas:
  - Presencia de bugs y vulnerabilidades
  - Aplicaciones y casas de cambio maliciosas
  - Publicar la cartera digital en RRSS
  - Realizar transacciones con carteras no fiables
  - Presiones regulatorias y normativas (AML, KYC, CTR)
- Acciones:
  - Análisis web (Búsqueda de información)
  - Análisis de la cadena de bloques
  - Monitorización de la red (P2P)
  - Uso de direcciones contaminadas (Marcado)
-

Usos del blockchain

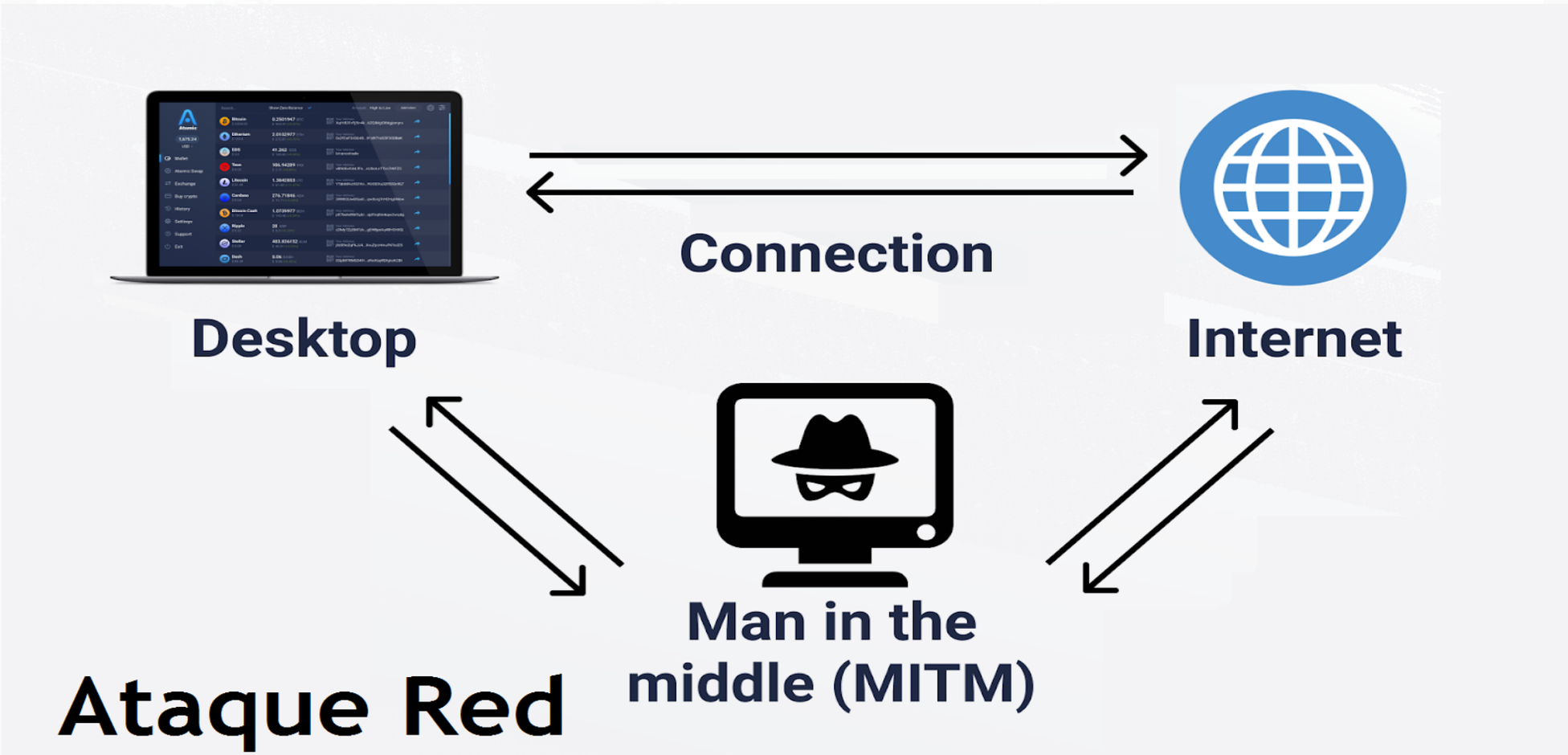
LEGALES

- Logística
- Trazabilidad
- Sector sanitario
- Propiedad intelectual
- Periodismo
- Otros...

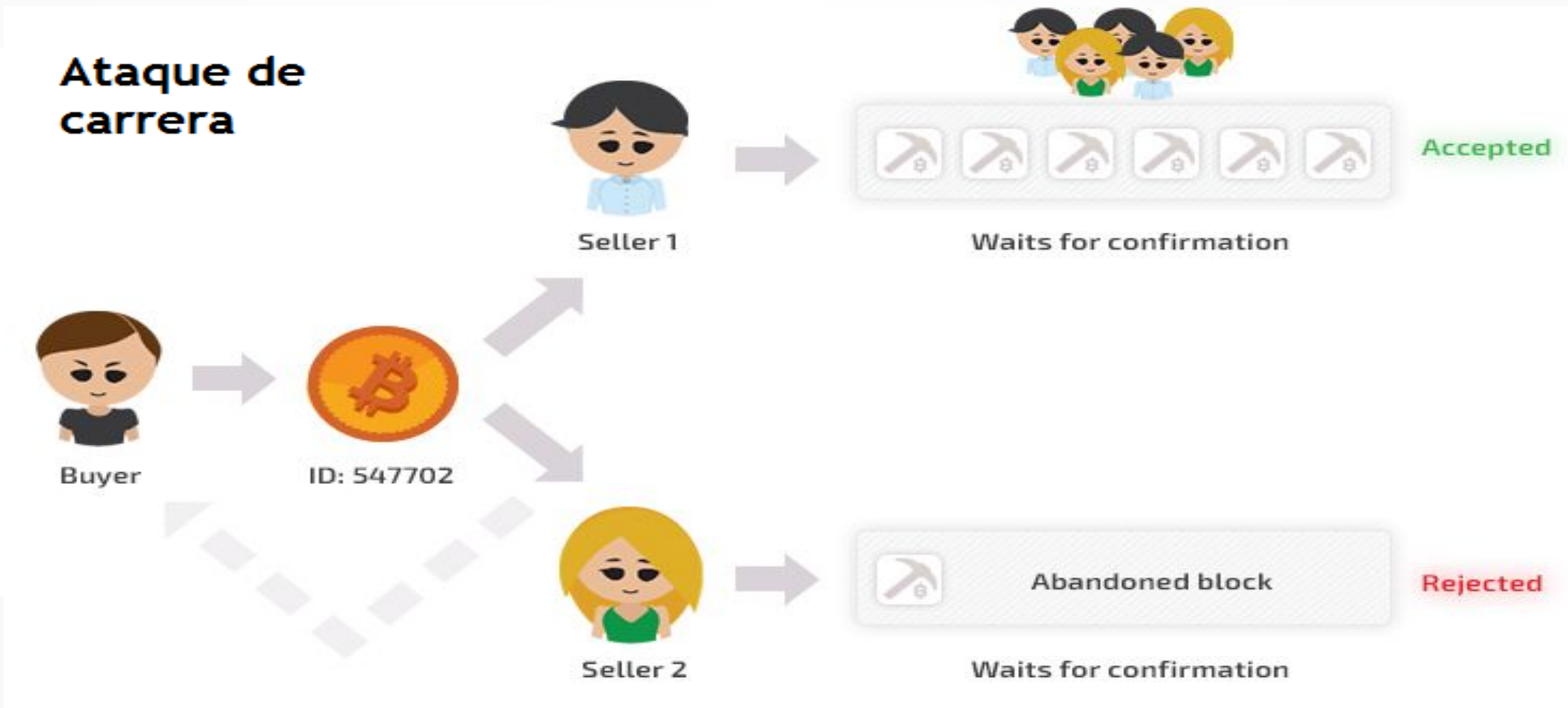
ILEGALES

- Pago por ransomware
- Cryptojacking
- Endpoint Miners
- Pagos en la *Darknet*
- Lavado de dinero
- Cebo en estafas

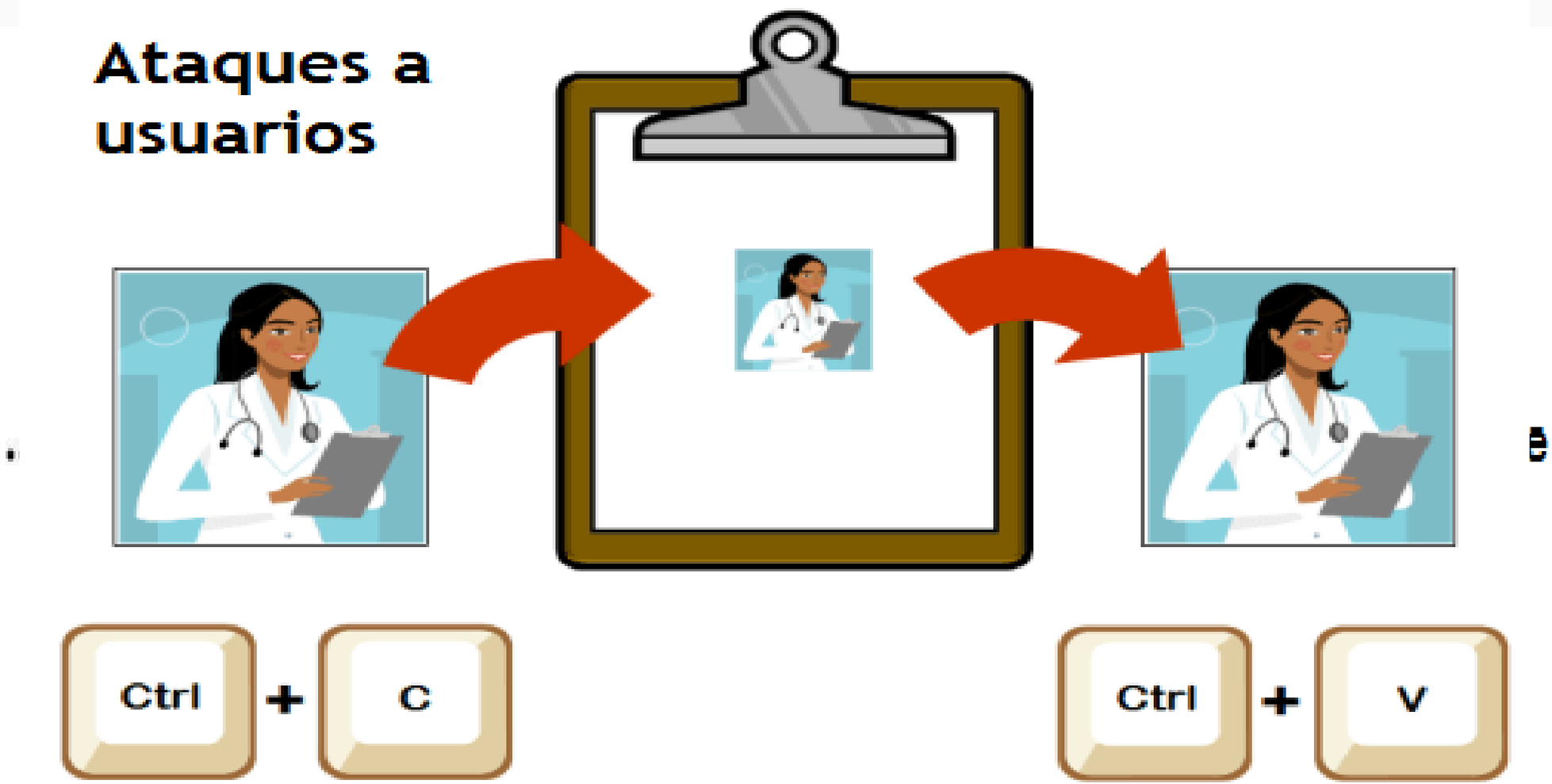
Amenazas y ataques I



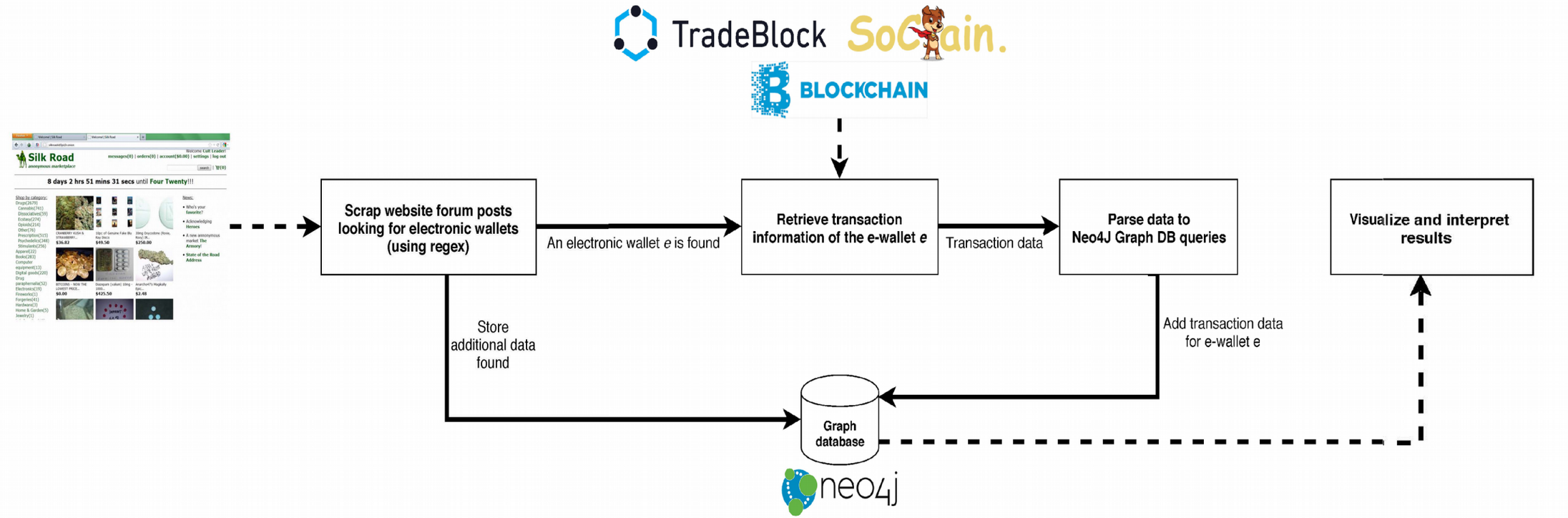
Amenazas y ataques II



Amenazas y ataques III

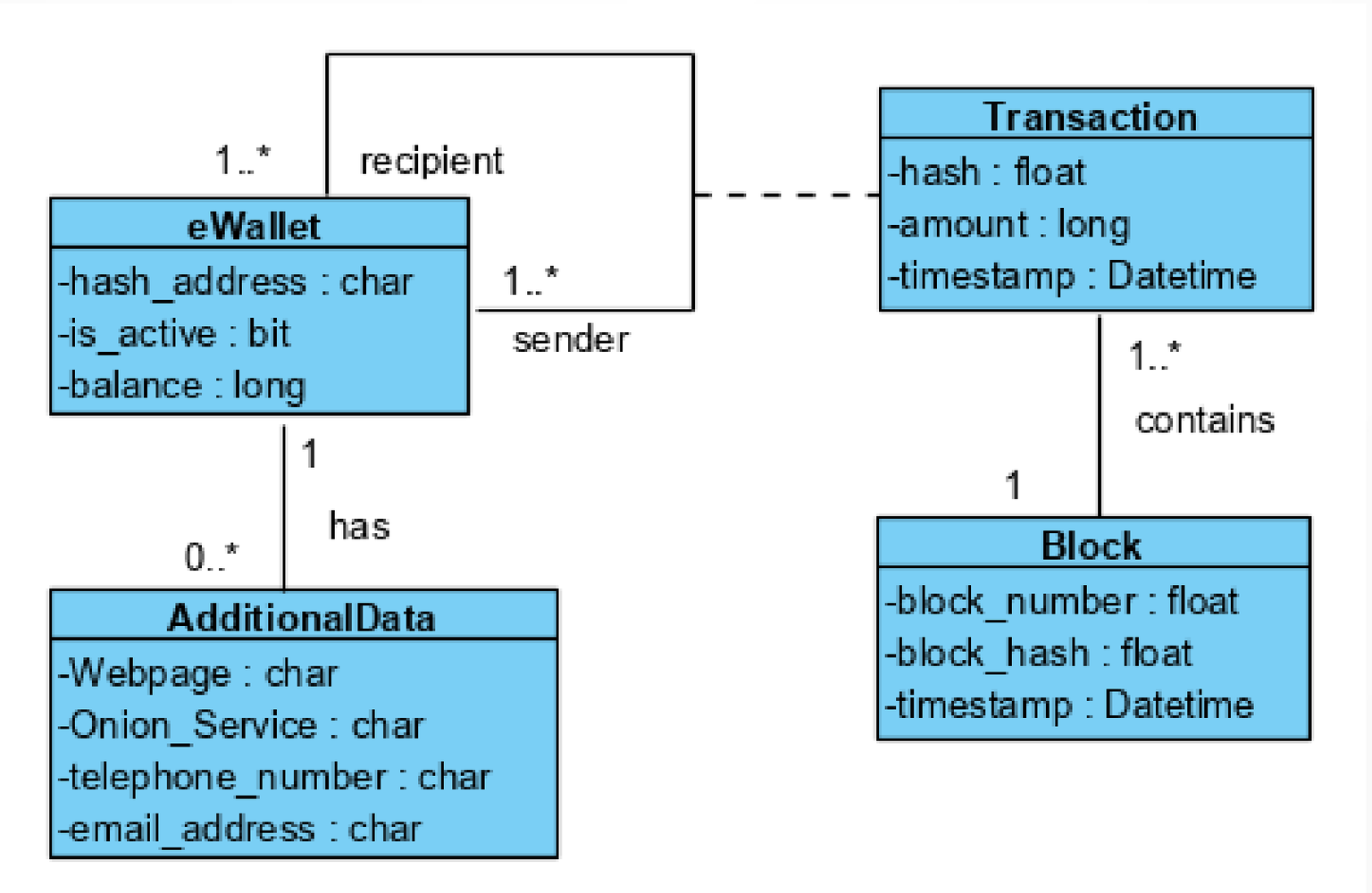


Sistema desarrollado



- Script de recolección y cribado de información
- Script de extracción de información de la cartera
- Script de visualización

Estructura BBDD sistema



Trabajo relacionado

- Dark Monitor de TNO Group
- Crystal de BitFury
- Chainalysis Reactor y KTC
- Crypto Forensics de Elliptic.co
- Coinfirm
- Coinbase Neutrino, etc...

Pero, ¿qué aporta esta herramienta?

Ventajas del sistema vs Competencia

- Código abierto y de carácter gratuito
- Permite realizar tareas elementales de análisis forense.
- Permite la detección de carteras digitales alojadas en Internet (en abierto o en la *Darknet)*
- Realiza consultas al ledger y obtiene información relativa a la cuenta detectada
- Establece las relaciones entre las diferentes carteras digitales

Conclusiones

- Estudio de los mecanismos de consenso
- Estudio de los vectores de ataque
- Diseño de un sistema de detección de carteras
- Extracción de información del blockchain
- Visualización de las relaciones entre las carteras

Líneas de mejora:

- Abstraer las acciones de recolección de información
- Incluir un detector de uso de carteras

Preguntas, por favor.

FIN