Seguridad Cripto Hacking

Los mayores robos de criptomonedas

En intercambios

Mt Gox 2014 Feb

FICHA

Ubicación: Japón , Shibuya

Monto robado: 850.000 bitcoin

Clientes afectados: 20.000

Fecha de evento: Febrero de 2014

Monto en USD para la fecha: 470 M USD

Monto actualizado: 50.000.000.0000 USD aproximado

Inicio mt gox

- Mt Gox fue fundado inicialmente en el año 2007 por el programador **Jed McCaleb**. En ese entonces funcionaba como un portal en línea para el intercambio de cartas del conocido juego **Magic: The Gatering**. De hecho, el nombre de Mt Gox era un acrónimo para **“Magic: The Gathering Online eXchange”.**
- Pero el uso y objetivo del sitio comenzaría a cambiar. En julio de 2010, McCaleb leyó sobre **Bitcoin** en Slashdot. Luego de conocer sobre la criptomoneda decidió que la comunidad de bitcoin necesitaba un intercambio. Esto con el fin de que sus usuarios pudieran comerciar bitcoin y otras monedas regulares. Fue así como el 18 de julio, McCaleb lanzó su servicio de intercambio y cotización de precios desplegándolo bajo el nombre de dominio mtgox.com.
- Sin embargo, para marzo de 2011, McCaleb vendió Mt. Gox al programador francés y entusiasta de Bitcoin, **Mark Karpeles**. Fue Karpeles quien se desempeñó como CEO de Mt Gox, convirtiéndose en su mayor accionista.

APOGEO

- Mt Gox dirigió el mayor volumen
- más de 127 mil usuarios activos por todo el mundo.
- 2011, Mt Gox comenzó a presentar varias vulnerabilidades y fallas graves de seguridad.
- Hackers hacen foco en el Exchange - ocasionan la pérdida de cientos de bitcoins durante 2011.
- Caída abrupta en los precios de Bitcoin dentro de la plataforma, pasando de los 17 $ USD a centavos.
- 2014 roban 850.000.
- Desestabilizó completamente el mercado de Bitcoin.

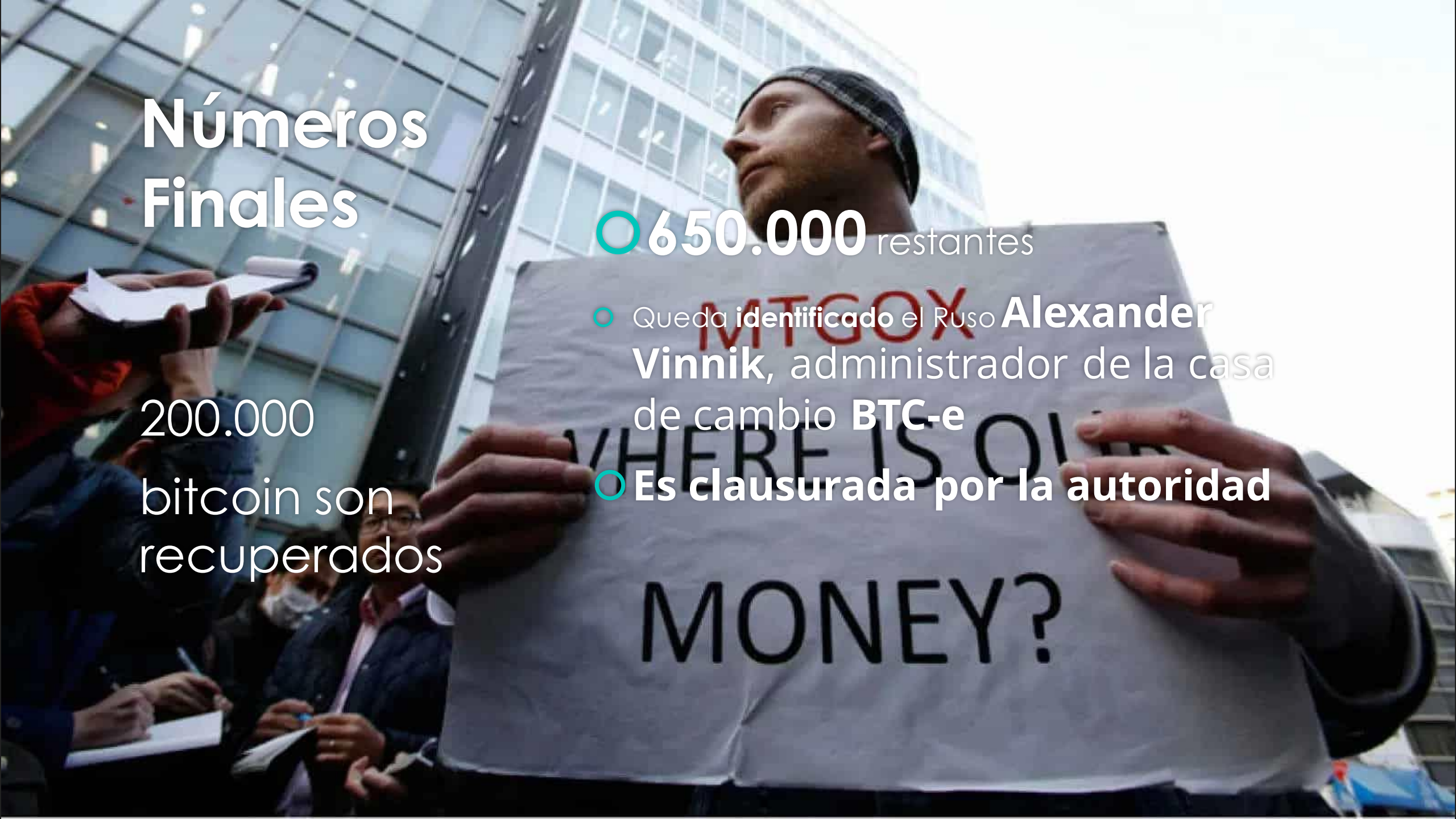
El Hackeo final 2014

- La clave privada del exchange Mt Gox quedó comprometida desde el primer hackeo ocurrido en 2011.
- En este primer hackeo se usaron las credenciales de un auditor de Mt Gox
- el hecho afectó a los usuarios por un total cercano a los 8,75 millones de USD.
- Posteriormente en 2013, se implementaron nuevas medidas de protección y seguridad.
- Aumenta usuarios y popularidad.
- en febrero de 2014 desaparecen más de 850.000 bitcoins.

Números Finales

200.000

bitcoin son recuperados



- **650.000** restantes
- Queda **identificado** el Ruso **Alexander Vinnik**, administrador de la casa de cambio **BTC-e**
- **Es clausurada por la autoridad**

Consecuencias Mt Gox

CONDENA

- Tanto el exchange Mt Gox, como su CEO y más de 20 mil usuarios y clientes, se vieron duramente afectados con dicho hackeo.
- Mark Karpeles fue acusado de malversación de fondos y manipulación de datos por la justicia japonesa.
- Los tribunales japoneses solicitaron que el CEO fuera condenado a 10 años de prisión. Aunque después de 11 meses, logró salir bajo fianza y estuvo a la espera de un juicio.
- Donde posteriormente fue declarado inocente de todos los cargos que se le acusaban.

CONEXIÓN

- Como cuestión informática los hechos reales no podrán ser determinados si fue hackeo o estafas encubiertas
- Las principales vulnerabilidades casi siempre surgen dentro de la seguridad de sistemas
- Continúan esperando el reembolso
- Finalmente identifican a **Alexander Vinnik**, como destinatario de los bitcoin en su intercambio

Seguridad Cripto Hacking BINANCE 2019

Los mayores robos de criptomonedas

En intercambios

BINANCE 2019 HACKING

- 7 de mayo de 2019
- el Exchange más importante del mundo
- robaron 40 millones USD (7.000 BTC).
- "alguien" ha hackeado el *hot wallet* de Bitcoin del Exchange (el monedero donde el Exchange guarda el dinero de los usuarios utilizado para trading intradía)

Binance no pudo determinar el modo

- desde Binance No saben cómo lo han hecho
- congelaron la retirada (withdraw) como el depósito de fondos, para que los nuevos fondos no se vean comprometidos
- se han aprovechado de vulnerabilidades de la API (las desconocemos) y han inyectado *malware* a través de mails internos a los propios empleados, con los que se han hecho con las claves de acceso (2FA) de las cuentas de usuarios y por lo tanto con el hot wallet de BTC.

Binance 2019 Hacking

Transacción Ver información de una transacción de Bitcoin

e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea

1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s 3CTPRyUbCKkByGmAVvDV6ReZXT1WfV3UPd	bc1qp6k6tux6g3gr3sxw94g9tx4l0cjtu2pt65r6xp	$ 3,228,385.46
	bc1qqp8pwq277d30cy7fjpvhcvhgztvs7v0nudgul5	$ 2,694,192.20
	32LZ4wWwEhTzwtqAm2gPauktYZb5kQ6C5a	$ 15.10
	3BMEXuoRza9EimRGSHGrwPmyFNUqWFpu8t	$ 433.47
	bc1qld27dqu6wrl4tmjdr8tl55qavmghwrr4ldh7qn	$ 2,752,257.00
	3BMEXtMSkRt3wwXKytg7Nj86utJeSbwFHx	$ 1,032.83
	bc1q8m9h3atn4cqeqhu3ekswdqxchp3g7d4v3qv3wm	$ 3,298,063.22
	14QZ2wB8b8ZQNgb978Lwptdc8Vhv5aZQM2	$ 112.89
	3L8JcsWNa3kuVaQJxAE1hhcoBT17rcJA6b	$ 86.72
	bc1q7p6edvd4zvtya8uj366c23dan8pvlp503spucu	$ 2,723,224.60
	bc1q93ecep2338dy9aauwyvh4g22t49rnedxl8z0tj	$ 1,158.39
	bc1ql0wlnu80l8kctjzkzlzd72sdjqwuvruvgepceq	$ 2,229,676.71
	bc1q3ldtrr6xtpx8jam5gw68aaexz2wtluj0qullvr	$ 1,103,225.39
	19GwykQiTA8PRD2vWJmRF8xiMdJw7SZZhU	$ 1,332.59
	1LmbAuieDKqZeQCUn8F5hrf87ocL3b1whA	$ 40.70
	3AiKChFEc5fpBvsi2Pr2YsFPWgrFeVQkXC	$ 111.23
	bc1qyv4zv0wjn299kx4yz6g7v6g6400wqgzcqgw9vx	$ 2,229,676.71
	17Bmh2aNne8sR9kRwMwDzWHAYeZaZPRm28	$ 13.09
	3DoSXzGZFbUnw4dC5Cwj7GZ7aKPLwFcKSg	$ 85.19
	3AoRjdkUFE4nfRtArRC8r1MnUjUPmuLdDP	$ 110.86
	3KBsR6Ld255Tw5hNR4S6KaX5SXxvRF6jv3	$ 7,546.57
	bc1q6fejm4r866tmt8ptf42juedv5gevlv2qt72agq	$ 2,159,998.95
	1L8ZtgE7tAuySsWhQn7SqdZwJPuMzqYmTx	$ 8.71
	1BsRYrL6FWjnX76nyvQUQXcv8QL2oZpJ6x	$ 121.36
	bc1qvstwzsrfml43jrclsp68220l4lx5lw3kwf7dp0	$ 1,126,451.31

Binance 2019 Hacking

- El propio CZ (CEO de Binance) ha dado la cara
- van a cubrir el robo con el "Fondo de Garantía de Depósitos" que constituyeron, donde disponen de liquidez suficiente.
- CZ "estamos heridos pero no acabados”";

Binance 2019 Hacking

- Los fondos robados representan el 2% del total de BTC que mantiene Binance
- si Binance movió en pleno *bull market* en 2018 unos 200mm USD por trimestre,
- El robo puede representar los beneficios del año

Seguridad Cripto Hacking Ethereum Classic Case

Los mayores robos de criptomonedas

THE DAO CASE

Ethereum Classic Case – 2016 THE DAO

- ETC es una blockchain
- origen en un hard fork
- el robo de varios millones de ethers en el año 2016
- resguardados por el proyecto The DAO
- dividió a la comunidad Ethereum entre quienes le apoyaban y detractaban.
- la mayoría aprobó su ejecución
- dividiendo a Ethereum en dos blockchain
- fondos robados fueron regresados a sus dueños en Ethereum
- Otra donde no se devolvió: Ethereum Classic.

Ethereum Classic Case – 2016 THE DAO

- mayo y junio de 2016
- proyecto **The DAO**, implementado como un **smart contract**
- llegó a tener un total de 11,5 millones de éter,
- **valorados en 150 millones de dólares para ese momento.**
- The DAO fue catalogado como el mayor evento de crowdfunding de la historia.
- El 30 de mayo de 2016, **Dino Mark**, **Vlad Zamfir** y **Emin Gün Sirer**, **publicaron** un informe sobre ciertas vulnerabilidades
- posibilidad, de explotar al menos nueve vulnerabilidades
- sus advertencias fueron desestimadas

Ethereum Classic Case – 2016 THE DAO

- el 16 de junio del 2016 se detectó un ataque sobre The DAO.
- Un grupo de hackers desconocidos movieron alrededor de 3,6 millones de Ether (equivalentes a unos 50 $ USD millones) de The DAO.
- El precio del Ether cayó de 20 $ USD a menos de 13 $ USD
- Debido al diseño de The DAO y el child DAO que usó el atacante, los fondos no se podían retirar antes de 28 días.
- Esto daba la oportunidad de recuperar los fondos.
- la comunidad Ethereum discutía si devolver o no, los fondos a los inversores y de qué manera lo harían.
- el 20 de julio de 2016, se produjo un hard fork con el fin de revertir el pirateo
- un grupo de personas apoyaba la idea de que la blockchain debería permanecer inmutable ante cualquier situación.
- Ethereum se dividió en dos.
- Ethereum, quedó bajo la tutela de Vitalik Buterin
- la original pasó a llamarse Ethereum Classic. Este proyecto continuó como un DAO,.

Ethereum Classic Case – 2016 THE DAO

- **Los principios de Ethereum Classic**

- **Inmutabilidad por sobre todas las cosas**
- La comunidad de Ethereum Classic cree que la principal propuesta de valor de cualquier blockchain es la inmutabilidad.
- Esto significa que las transacciones válidas nunca pueden ser borradas u olvidadas.
- Los individuos que interactúan en Ethereum Classic se rigen por esta realidad.
- la frase: **“El Código es la Ley.” CODE IS LAW**

Ethereum Classic Case – 2016 THE DAO

- **Los principios de Ethereum Classic**

- **Gobernanza descentralizada**
- Otro punto que desea la comunidad de Ethereum Classic es que se respete en todo momento la gobernanza descentralizada.
- Su visión en este aspecto, es que solo la descentralización puede garantizar la vida del proyecto más allá del tiempo.
- Además, indican que la descentralización evita la corrupción, irresponsabilidad, nepotismo, ineficiencia y el estancamiento.
- Ethereum Classic manifiesta estos valores renunciando al control por una base central formalizada.
- La única jerarquía es la de la meritocracia transparente y la reputación mutua.

Ethereum Classic Case – 2016 THE DAO

- **ETHEREUM VS ETHEREUM CLASSIC**
- **SIMILITUDES**
- Protocolo **POW**
- algoritmo **Ethash.**
- **UTILIZA EVM (Ethereum Virtual Machine)**
- significa que Ethereum Classic puede desplegar smart contracts, DApps.
- capacidad de emitir tokens compatibles con el estándar **ERC-20**

- **DIFERENCIAS**
- límite de emisión Ethereum Classic **máxima de 230 millones**
- Ethereum esta es infinita
- Recompensa de minería, mayor en Ethereum Classic, 4 Ethers por bloque.

Seguridad Cripto Hacking

Los mayores robos de criptomonedas

En intercambios

Muchas Gracias por compartir el conocimiento entre todos

Criptomonedas

en definitiva
significa

Libertad