CURSO
BLOCKCHAIN

Modulo 2

Historia

Lo visto

Estudiamos:

- Sistemas numéricos: Bit, Hexadecimales
- Matemática: Lógica, funciones
- Arquitectura de computadoras: Algoritmos, memoria volátil, memoria no volátil.
- Criptografía: Hash, criptografía simétrica y asimétrica.
- Seguridad: Usando la criptografía como resguardo de privacidad e integridad
- Ataques: Ciber delitos para violentar la privacidad e integridad de las personas y empresas.

CURSO BLOCKCHAIN

Historia (40m)

1. **Cronología:** Atbash, Cifrado Cesar, Cifrado de Viginere, Criptosecretismo, cryptografía asimetrica, MD4(1980) ⇒MD5⇒SHA1⇒SHA2⇒SHA3 (2012) (5')
2. **Vocabulario**: SHA, NIST, ITAR, Gran Hermano (2')
3. **criptoguerra**: Cypherpunks, David Chaun, Tim May (manifiesto criptoanarquista), Eric Hugh (manifesto cypherpunk), Phill Zimmermann (PGP+ Cargos terroristas), Joe Biden (Propuesta de guerra contra terrrorismo), Intel (Cliper chip) y Matt Blaze, fin de criptografía en ITAR, Contrataque cypherpunk, Jim bell, Julian Assange. (20')
4. **Comienzo de criptomonedas**: Ecash (David Chaun), bmoney (weidai), Finney (PoW+Bitcoin), Szabo (smart contracts, timestamp), Satoshi Nakamoto (Cryptography mailing list), Silkroad, Proyectos de ex-cypherpunks (Blockstream, elixir, CASA, BitTorrent, Zcash). (10')
5. **Smart contracts**: Szabo, Vitalik Buterin (Ethereum), Charles Hoskinson (Cardano), BSC, Polkadot, algorand, solana, terra. (3')

CURSO BLOCKCHAIN

Cypherpunks

Entendiendo espíritu de la blockchain

Vocabulario

Encriptar o cifrar: *Volver ilegible algún mensaje. (Desencriptar o descifrar es el proceso inverso)*

Hash: *Función que ante una entrada específica devuelve un conjunto único de caracteres distintos pero de igual longitud.*

SHA: Algoritmo de hash criptográfico de Secure Hash Algorithm.

NIST: Instituto Nacional de Estándares y Tecnología. (encargados de estandarizar los algoritmos de SHA)

ITAR: Reglamento Internacional de Armamento.

NSA: La Agencia de Seguridad Nacional (NSA) es una agencia gubernamental de inteligencia de los Estados Unidos responsable de la recopilación, análisis y protección de la información comprometedora de los Estados Unidos. También opera sistemas de vigilancia de telecomunicaciones para monitorear el tráfico de datos a nivel mundial.

Gran Hermano: Organización grande que puede o usa tus datos para algún beneficio de ellos. (Gobierno, redes sociales, etc).

Smart Contracts: Programas que corren deterministicamente y no pueden ser alterados. Esto lo hacen aprovechando las características de la blockchain.

CURSO BLOCKCHAIN

Historia

Atbash

Jeremías 25:26. Sheshakh en vez de decir Babilonia.

Cifrado de Viginere

Con clave de cifrar y descifrar cíclica. (Lo usan los Nazis en la 2da guerra mundial)

Avances Criptografía

1) Criptografía asimetrica
2) David Chaun (Comunicacion, Identidad, Dinero)

Inflexion

1) Zimmermann - ciberterrorista.
2) Joe Biden- antiterrorismo (91)
3) Smart Contracts (93-94 - Szabo)
4)Cliper chip (94) - Matt Blaze
5) 1996 cancelan cliper chip y juicio a Zimmermann.
6) 1997 - ITAR
7)Assesination politics
8) Echash (digicash)- 98 al 99.
9) Bmoney (WEIDAI - 98)

Bitcoin

1) Silkroad (Ross Ulbricht- 2011-2013)
2) Proyectos variados de cypherpunks (blockstream, elixir, zcash, bit-torrent, Casa)
3) Ethereum (Vitalik Buterin -2013-2015)
4) Cardano (Charles Hoskinson 2015)
5) DAO Hack (2016)
6) Algorand (2019 - Silvio Micali)
7) Terra (Do kwon- 2019)

VI ac | I ac | XVI dc | 50' 60' | 70' | 80' | 90' | 2000' | 2010' | 2020'

Cifrado Cesar

Con clave para cifrar y descifrar.

Criptosecretismo

Solo la NSA y estados fuertes. Prohibida para civiles y consideradas armas militares (ITAR).

Cypherpunks

1) Manifiesto Criptoanarquista (Tim May)
2) Manifiesto Cypherpunk (Eric Hugh)
3) PGP (pretty good privacy, Zimmermann)

Ataque

1)Hashbash (Adam Back 2002)
2) Reinventa PoW (Finney 2004)
3) Timestamp (Szabo - 2005)
3) Conspirancy as govern (Julian Assange 2006)
4) Bitcoin (2008 - Satoshi Nakamoto)

Escalamiento

1) BSC, polkadot, solana, polygon, Starknet
2) The Merge (2022)

Bitcoin pizza day

22 de Mayo de 2010.

El programador estadounidense Laszlo Hanyecz realizó en Florida, Estados Unidos, la primera transacción comercial con Bitcoin (BTC) y pagó dos pizzas grandes de muzzarella de la cadena Papa John's un valor de 10.000 bitcoins.

Hoy se recuerda ese día cada año.

Cypherpunks para investigar

Adam Back - @adam3us	Bram Cohen - @bramcohen
Nick Szabo - @NickSzabo4	Zooko Wilcox - @zooko
David Chaum - @chaumdotcom	Matt Blaze - @mattblaze
Hall Finney - @halfin	Matthew Green - @matthew_d_green
Jameson Lopp - @lopp	Runa Sandvik - @runasand
Eva Galperin - @evacide	

Competencia ethereum

Cardano: permite multichain y smart contract, son más rapidas que ethereum pero tiene menos años en el mercado y hay una organizacion que lidera (con un cofundador de eth)

Ethereum: es single chain, smart contract, la primera en su clase. Es lenta pero se está trabajando para remediarlo. el proyecto lo lidea la comunidad abierta y no una empresa. para multichain hay que implementar bridges.

BSC: es mas escalable y barato que ethereum pero más centralizado.

Polkadot: creado por inventor de solidity. Es multichain por excelencia y 10mil transacciones por segundo

Algorand: busca ser descentralizada, 10mil transacciones por segundo, fue destacada por vitalik buterin, pero la verdad pocos la usan.

Solana: la blockchain más rápida (50k transacciones x s)

Terra: protocolo para fortalecer la infraestructuras de las stablecoins y las defi, aunque el año pasado se dio una corrida bancaria que las desestabilizo.

Futuro de Smart Contracts

Historiales médicos
Registro de inmuebles
registro de títulos
patentes y propiedad intelectual
Votaciones (España -> Identidad digital)
Seguros (determinar pólizas automáticamente, efectuar pagos)

CURSO BLOCKCHAIN

Bibliografía

David Chaum: https://chaum.com/security-without-identification/

Manifiesto cryptoanarquista: https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

Manifiesto CypherPunk: https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt

PGP: https://shrinke.me/PdZ9

RSA: https://drive.google.com/file/d/1BTD9I5aoDmKBM8hJ97R5hQDP_TZRvAki/view

Criptografía general: https://drive.google.com/file/d/1MGMLOiWxxtqtTH7VxqHPikPnB4-IKA11/view

Clipper chip: https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

Assassionation Politics: https://cryptome.org/ap.htm

Bmoney: http://www.weidai.com/bmoney.txt

PoW: https://nakamotoinstitute.org/finney/rpow/

Bitcoin whitepaper: https://bitcoin.org/bitcoin.pdf

Resumen

1) **Cypherpunks:** Grupo criptoanarquista que culminó en la creación de dinero digital para resguardo de la privacidad de los rebeldes ante el gran hermano.
2) **Ecash:** Primer criptomoneda creada pero fracasa
3) **Bitcoin:** Primera criptomoneda creada por Satoshi Nakamoto, inspirada de Bmoney que resuelve problemas tecnológicos hasta el momento de lo que sería la tecnología blockchain.
4) **Ethereum:** Blockchain inspirada de bitcoin que agrega la posibilidad de smart contracts. Aunque es la primera, no es la única.
5) **Avances criptográficos:** Cómo prosperó en el tiempo, siendo muy poco usado hasta las 2da guerra mundial, permaneciendo luego en secreto para las fuerzas militares con increíbles avances como la criptografía de clave pública y peleada por los cypherpunks para su utilización civil, lo cual termina con el triunfo cypherpunk y siendo la base de la blockchain y las criptomonedas.

Consultas

¿?

Reto

https://cursoblockchain.com.ar/

CURSO BLOCKCHAIN

Actividad

1) Ordenar cronológicamente
   a) Silkroad
   b) Ecash
   c) The Merge
   d) exclusión de criptografía como arma militar
   e) DAO hack
   f) ethereum
   g) Atbash
   h) Wikileaks
   i) Cripto Secretismo
   j) Bmoney
   k) Cifrado Cesar
   l) nacimiento Cypherpunks
   m) Cifrado Viginere
   n) Bitcoin
   o) RSA