Blockchain Academy México

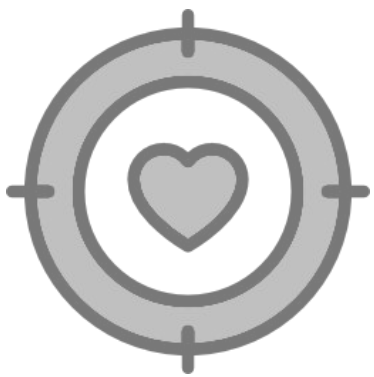
Blockchain 101

Módulo 0

BLOCKCHAIN ACADEMY MÉXICO

¿En qué nos enfocamos?

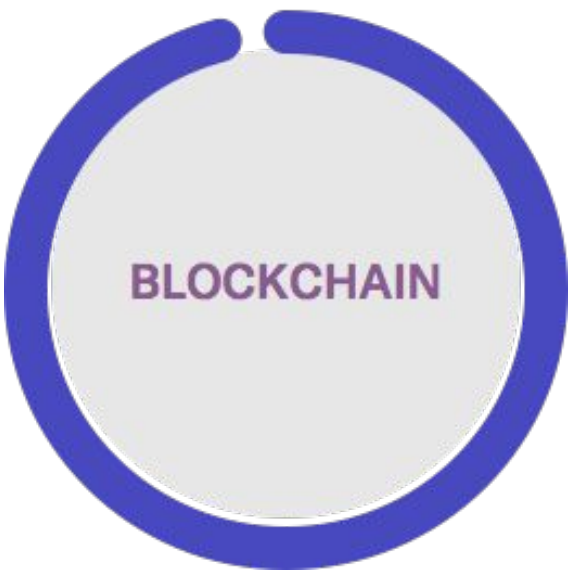
Objetivo del curso



- Profundizar en el funcionamiento del Blockchain
- Desarrollar capacidad de análisis para la implementación de la tecnología

De lo que **NO** vamos a hablar

De lo que **SI** vamos a hablar



Recursos

Link de carpeta

Comunicación

URL: blockdemy

URL

Herramienta

METAMASK

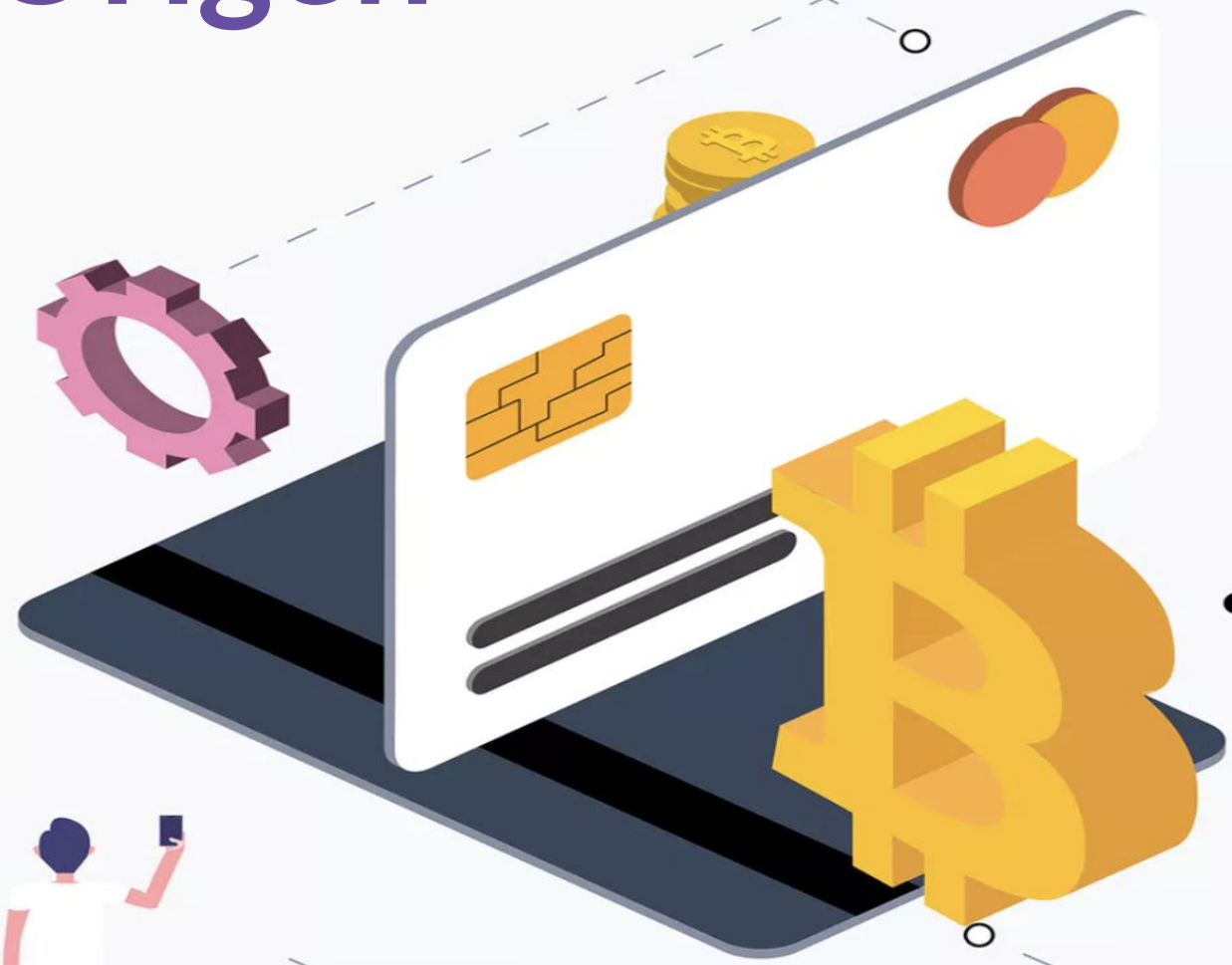
¿Por qué aprender blockchain?

Impacto mediático

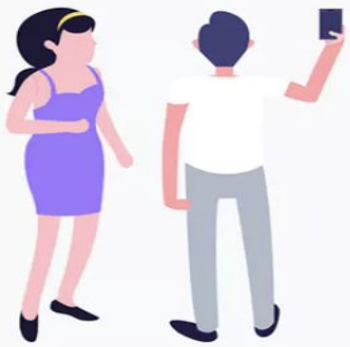
Así nos podríamos sentir pero en el 2019

Origen

Pérdida de la confianza



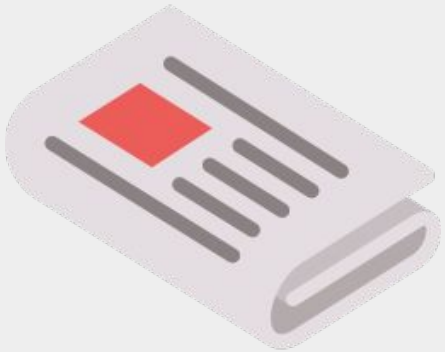
Criptografía



Cypherpunks

Internet

Búsqueda de la **democratización** de la información

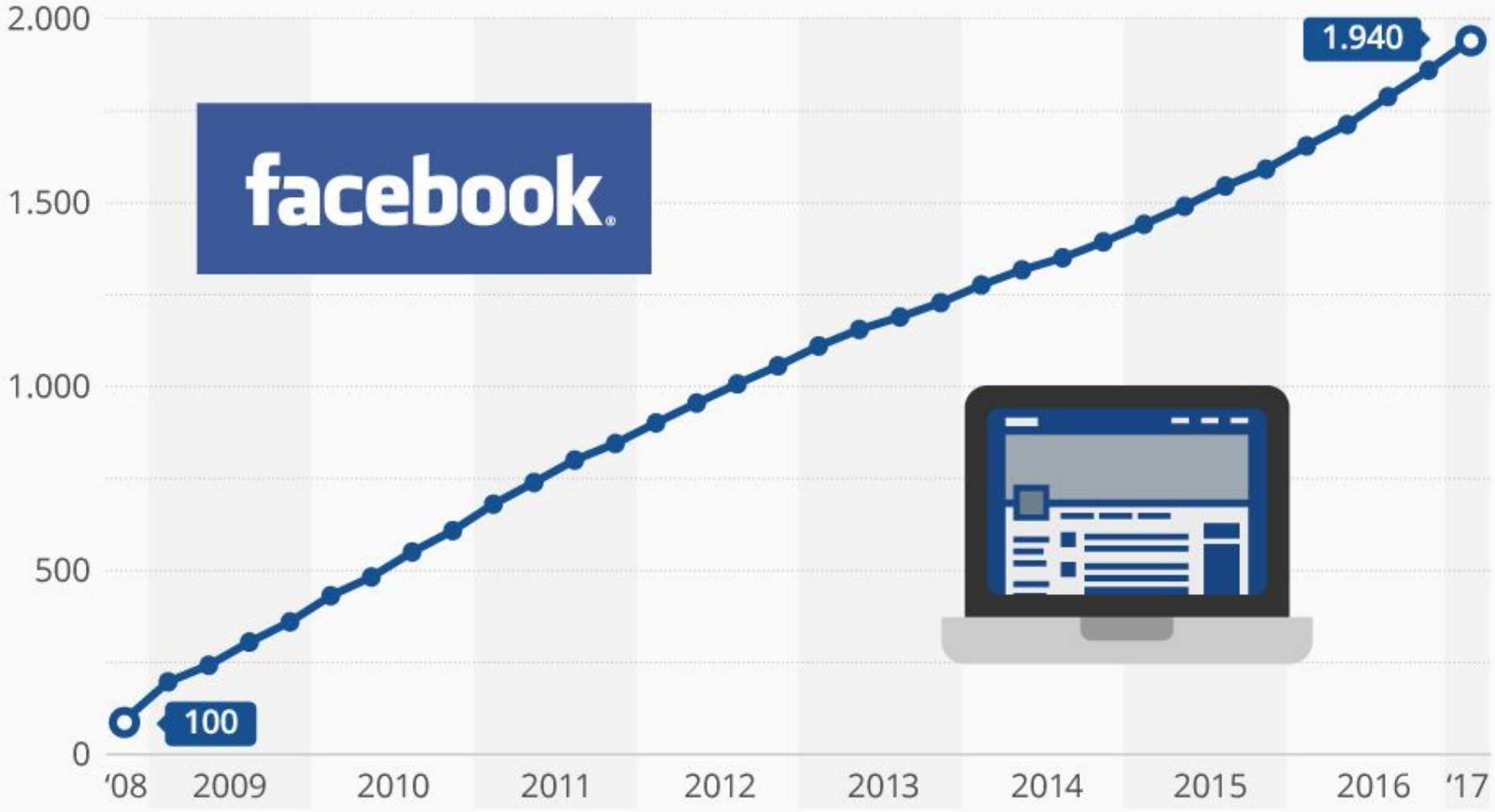


¿Problemas con el internet?

El flujo de la información pasa por sólo un PUNTO bajo el control de unos cuantos.

Facebook, muy cerca de los 2.000 millones

Usuarios activos mensuales de Facebook (en millones)*



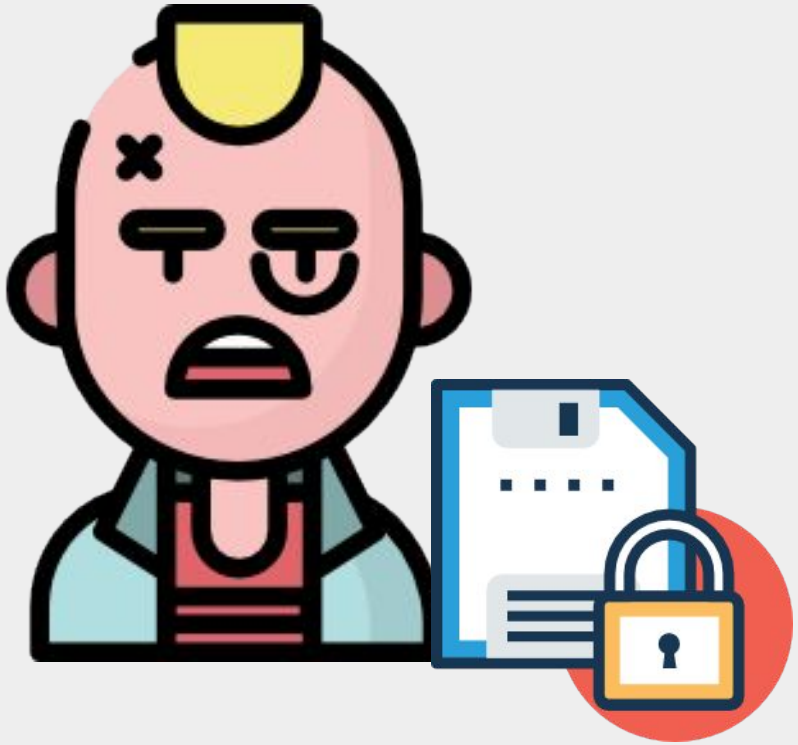
* Usuarios que se han registrado a la red social Facebook en los últimos 30 días.

Fuente: Facebook

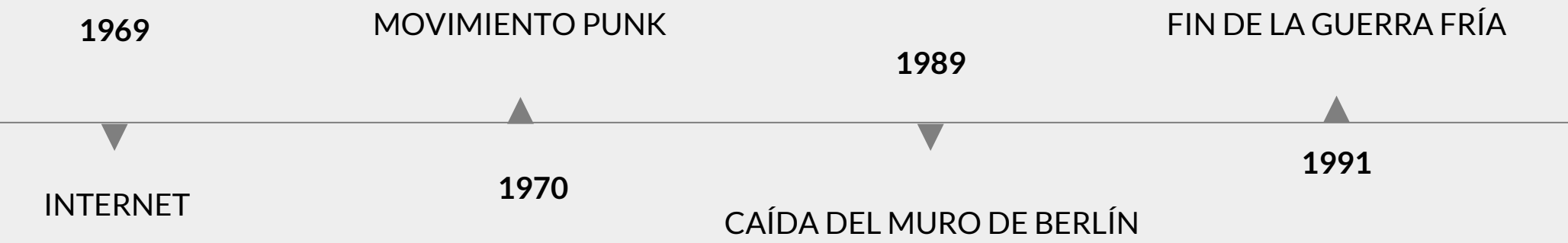
Contrastes

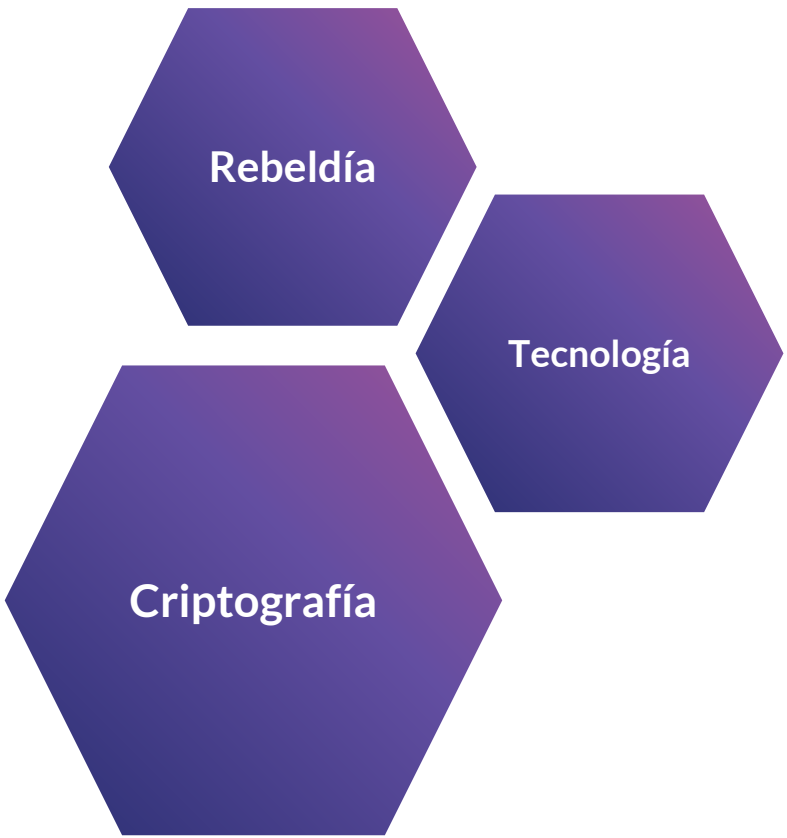

Internet 2.0
Compartir información
Transferir valor o activo
Blockchain

Cypherpunks



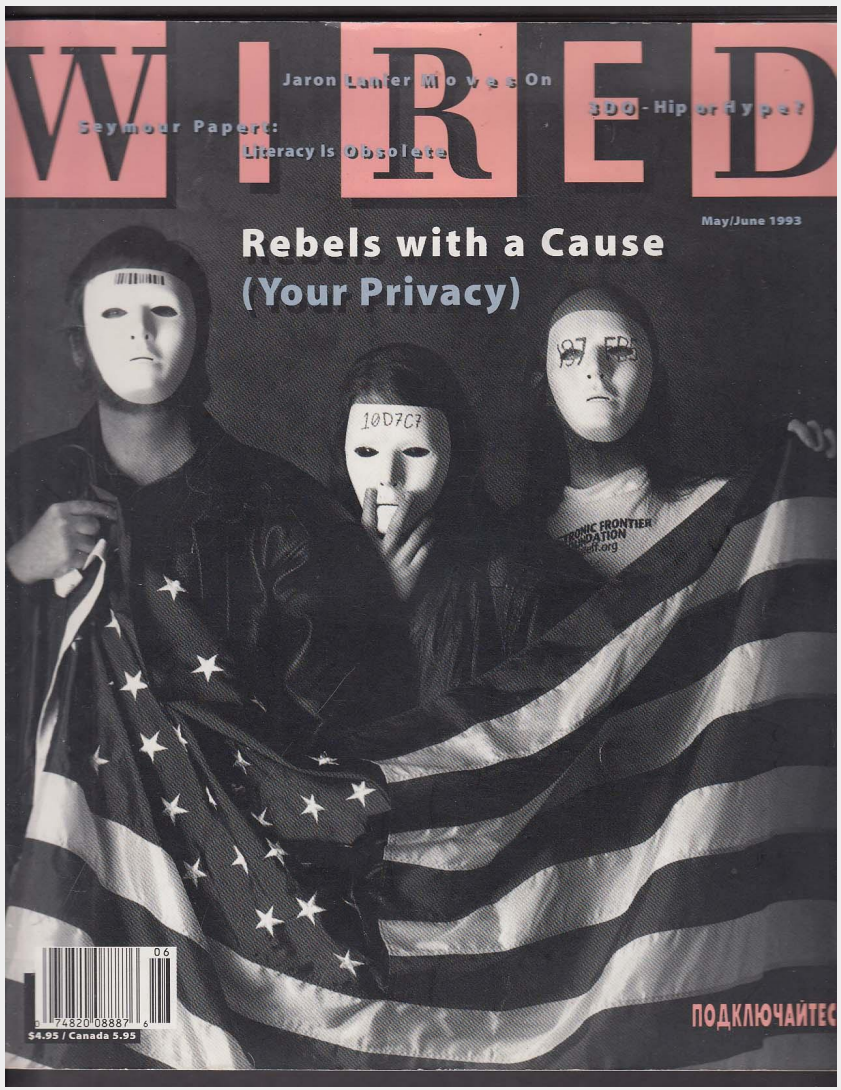
Antecedentes de los Cypherpunks





= Cypherpunks

1991



El problema: falta de privacidad y comunicaciones **no** seguras

Se libera el **cifrado asimétrico**

Se crean los cypherpunks

Objetivo: resistir a la pérdida de la privacidad del usuario en la era digital/internet

4 PUNTOS

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A pr
something one doesn't want anybody to know. Privacy is the power to selectively reveal o

If two parties have some sort of dealings, then each has a memory of their interaction. Ea
could pass laws against it, but the freedom of speech, even more than privacy, is fundame
together in the same forum, each can speak to all the others and aggregate together knowl
enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge
spoken of, we must ensure that we reveal as little as possible. In most cases personal iden
is no need to know who I am. When I ask my electronic mail provider to send and receive
what others are saying to me; my provider only need know how to get the message there
mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I

Therefore, privacy in an open society requires anonymous transaction systems. Until now
transaction system. An anonymous system empowers individuals to reveal their identity v

fuente:
https://www.activism.net/cypherpunk/manifesto.html

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A pr
something one doesn't want anybody to know. Privacy is the power to selectively reveal o

If two parties have some sort of dealings, then each has a memory of their interaction. Ea
could pass laws against it, but the freedom of speech, even more than privacy, is fundame
together in the same forum, each can speak to all the others and aggregate together knowl
enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge
spoken of, we must ensure that we reveal as little as possible. In most cases personal iden
is no need to know who I am. When I ask my electronic mail provider to send and receive
what others are saying to me; my provider only need know how to get the message there
mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I

Therefore, privacy in an open society requires anonymous transaction systems. Until now
transaction system. An anonymous system empowers individuals to reveal their identity v

1 La privacidad **es necesaria** para una sociedad abierta en la era electrónica

2 Privacidad !== Secretismo

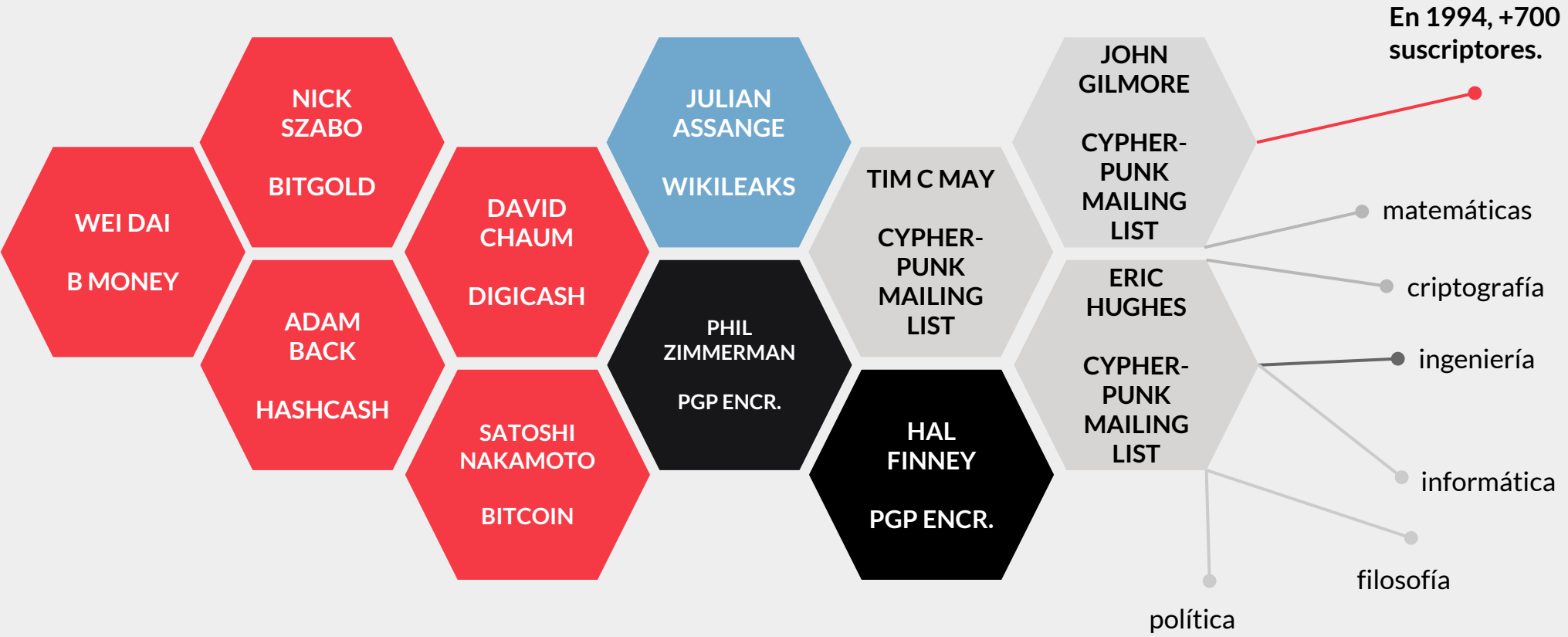
3 La privacidad es **la capacidad de revelarse selectivamente** al mundo

4 La privacidad en una sociedad abierta **requiere sistemas anónimos** para efectuar transacciones.

transacciones anónimas !== secretas

fuente:
https://www.activism.net/cypherpunk/manifesto.html

Cypherpunks



DiGi CA.SH®
MOBILE PAYMENTS

1983

Algoritmo RSA

El banco central, lo absorbe

Microsoft intenta comprarlo

1998

Bancarrota

Hash-Cash

ADAM BACK

Actualmente es el líder del proyecto **Blockstream.**

Hashcash fue una propuesta realizada por **Adam Back** para combatir el correo basura o spam.

Un **Sistema de prueba de trabajo** o **Sistema "POW"** (del inglés *Proof-Of-Work system*), es un sistema para evitar comportamientos indeseados.


BLOCKCHAIN
ACADEMY
MÉXICO