

Blockchain Academy México

Blockchain 101

Módulo 0

¿En qué nos enfocamos?

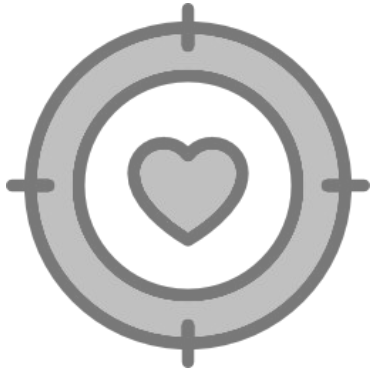
Aquí el futuro



Esperanza

Exageración

Objetivo del curso

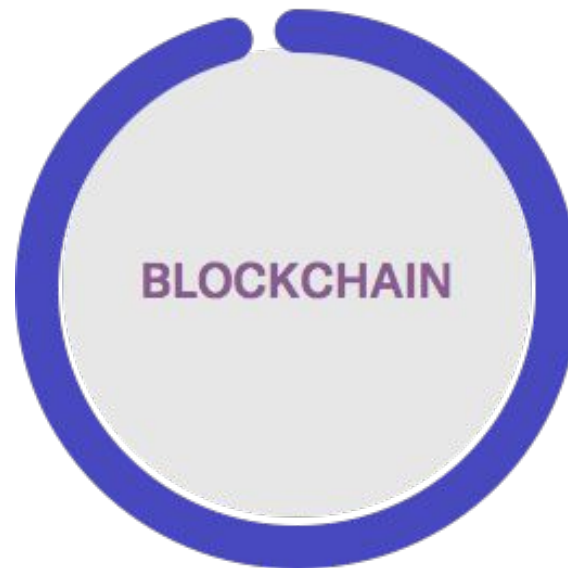


- Profundizar en el funcionamiento del Blockchain
- Desarrollar capacidad de análisis para la implementación de la tecnología

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?***



1	100	100	100	100	100
2	100	100	100	100	100
3	100	100	100	100	100
4	100	100	100	100	100
5	100	100	100	100	100
6	100	100	100	100	100
7	100	100	100	100	100
8	100	100	100	100	100
9	100	100	100	100	100
10	100	100	100	100	100
11	100	100	100	100	100
12	100	100	100	100	100
13	100	100	100	100	100
14	100	100	100	100	100
15	100	100	100	100	100
16	100	100	100	100	100
17	100	100	100	100	100
18	100	100	100	100	100
19	100	100	100	100	100
20	100	100	100	100	100
21	100	100	100	100	100
22	100	100	100	100	100
23	100	100	100	100	100
24	100	100	100	100	100
25	100	100	100	100	100
26	100	100	100	100	100
27	100	100	100	100	100
28	100	100	100	100	100
29	100	100	100	100	100
30	100	100	100	100	100
31	100	100	100	100	100
32	100	100	100	100	100
33	100	100	100	100	100
34	100	100	100	100	100
35	100	100	100	100	100
36	100	100	100	100	100
37	100	100	100	100	100
38	100	100	100	100	100
39	100	100	100	100	100
40	100	100	100	100	100
41	100	100	100	100	100
42	100	100	100	100	100
43	100	100	100	100	100
44	100	100	100	100	100
45	100	100	100	100	100
46	100	100	100	100	100
47	100	100	100	100	100
48	100	100	100	100	100
49	100	100	100	100	100
50	100	100	100	100	100
51	100	100	100	100	100
52	100	100	100	100	100
53	100	100	100	100	100
54	100	100	100	100	100
55	100	100	100	100	100
56	100	100	100	100	100
57	100	100	100	100	100
58	100	100	100	100	100
59	100	100	100	100	100
60	100	100	100	100	100
61	100	100	100	100	100
62	100	100	100	100	100
63	100	100	100	100	100
64	100	100	100	100	100
65	100	100	100	100	100
66	100	100	100	100	100
67	100	100	100	100	100
68	100	100	100	100	100
69	100	100	100	100	100
70	100	100	100	100	100
71	100	100	100	100	100
72	100	100	100	100	100
73	100	100	100	100	100
74	100	100	100	100	100
75	100	100	100	100	100
76	100	100	100	100	100
77	100	100	100	100	100
78	100	100	100	100	100
79	100	100	100	100	



Así nos podríamos sentir pero en el 2019





Origen

Pérdida de la confianza

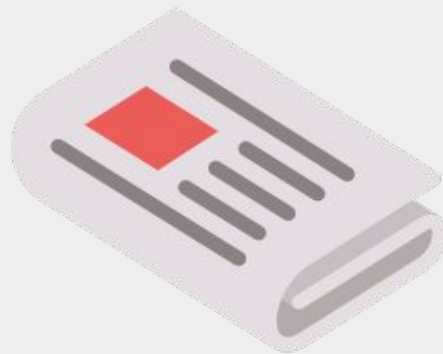


Cypherpunks

Internet



Búsqueda de la **democratización** de la información



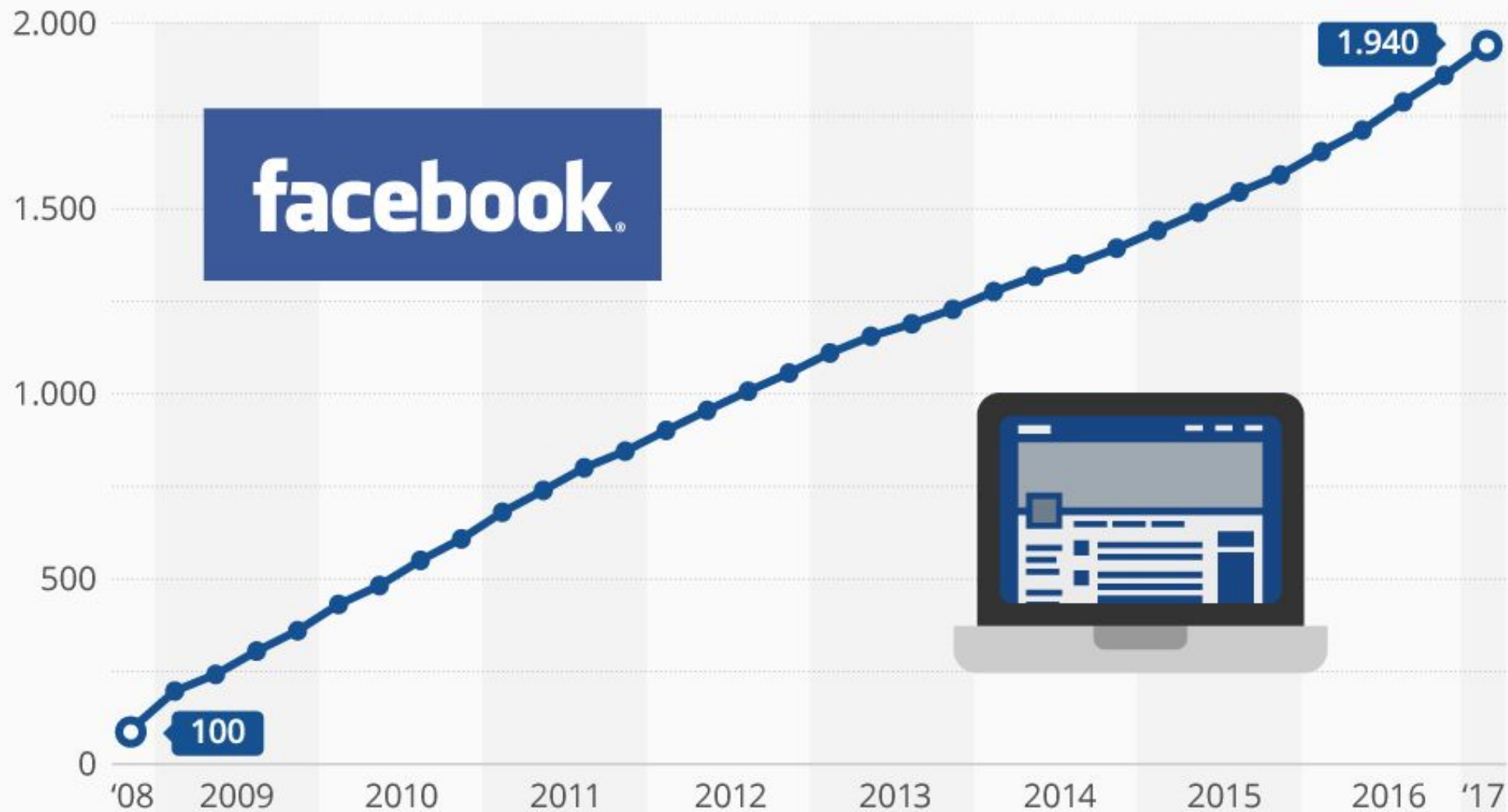
¿Problemas con el internet?

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)*



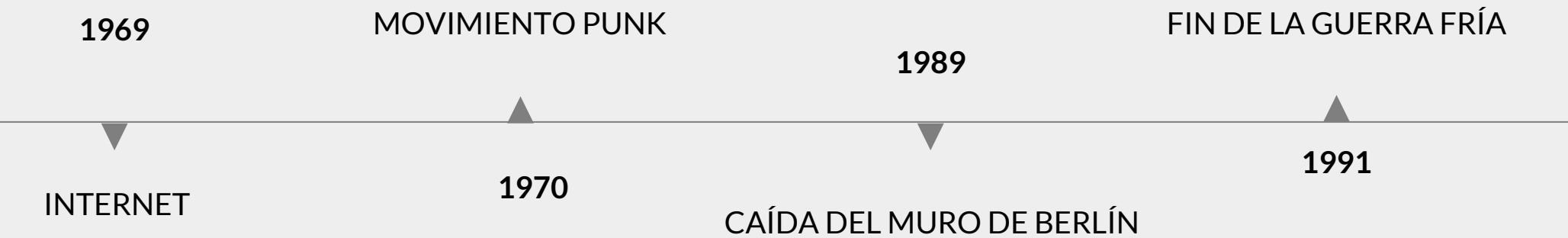
Contrastes

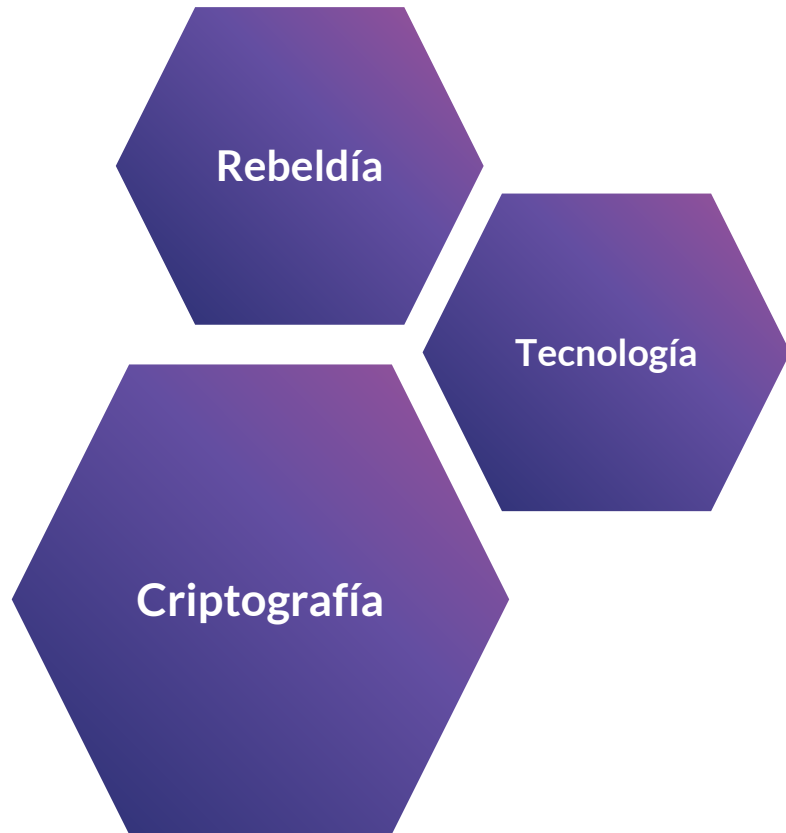


Cypherpunks



Antecedentes de los Cypherpunks



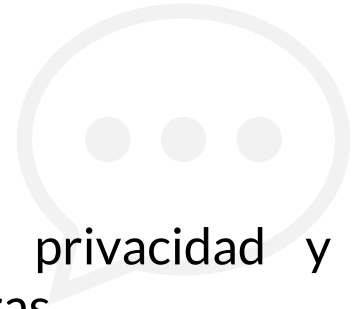


=

Cypherpunks



1991

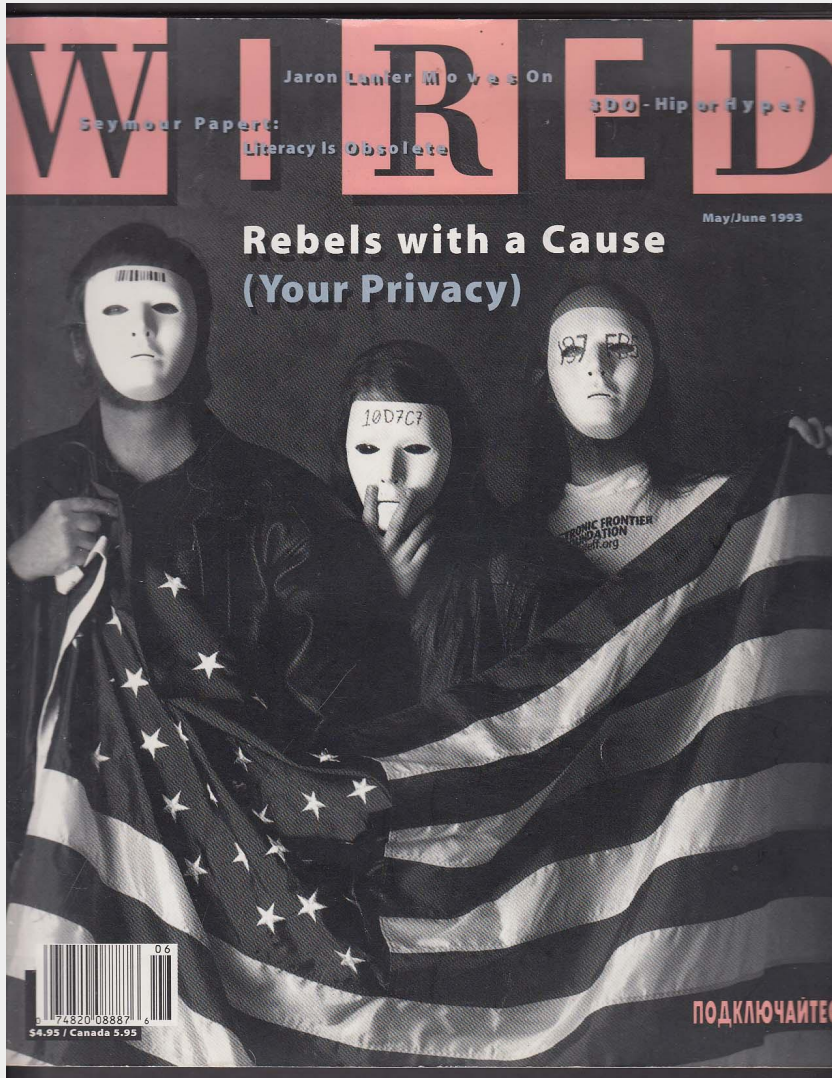


El problema: falta de privacidad y comunicaciones no seguras

Se libera el **cifrado asimétrico**

Se crean los **cypherpunks**

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



by [Eric Hughes](#)

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

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

A Cypherpunk's Manifesto

by [Eric Hughes](#)

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private thing isn't secret because somebody else has to know it. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society. In the same forum, each can speak to all the others and aggregate together knowledge. 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 of the transaction. If we are spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not needed to know who I am. When I ask my electronic mail provider to send and receive messages for me, my provider only needs to know how to get the message there and the mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must reveal all.

Therefore, privacy in an open society requires anonymous transaction systems. Until now there has been no such transaction system. An anonymous system empowers individuals to reveal their identity to the world.

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.



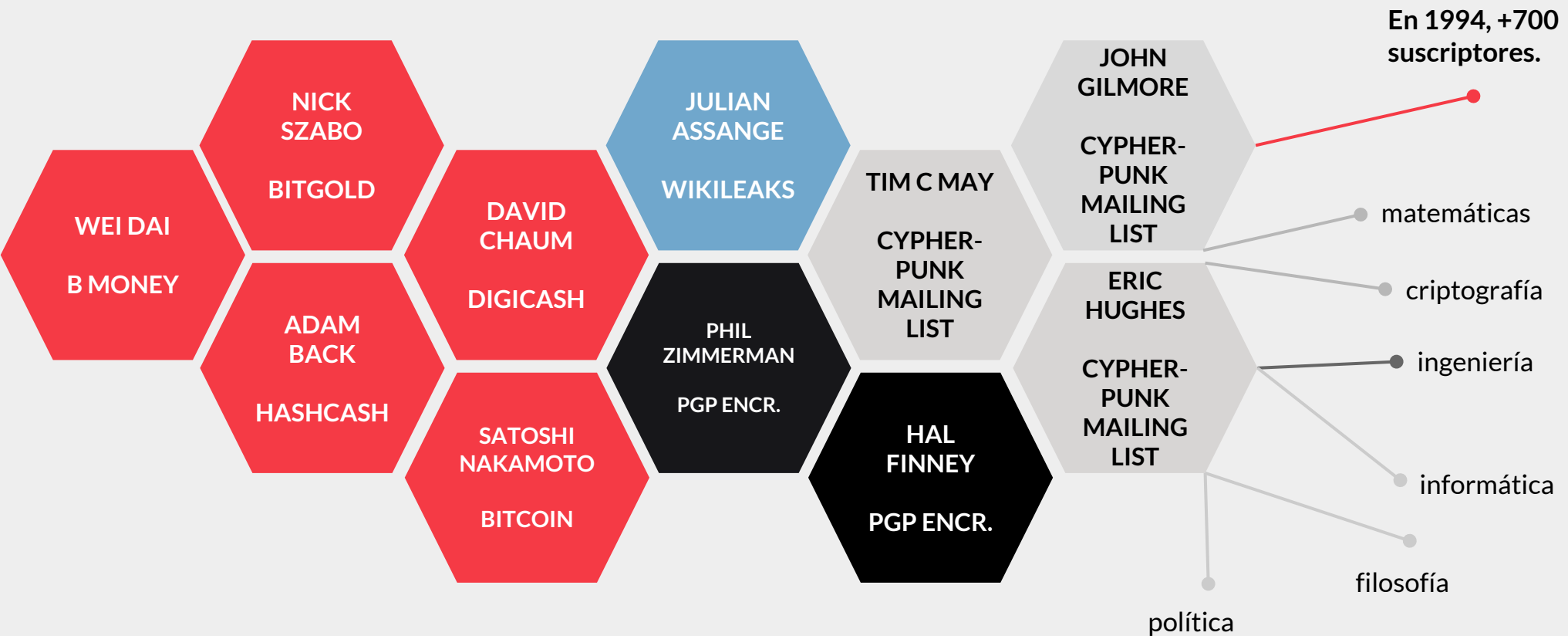
transacciones anónimas **!=** secretas

fuentes:

<https://www.activism.net/cypherpunk/manifesto.html>



Cypherpunks





1983

Algoritmo
RSA

El banco central, lo
absorbe

Microsoft intenta
comprarlo

Bancarrota

1998



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