

A LA DÉCOUVERTE DES BLOCKCHAINS PUBLIQUES

Consultant Blockchain

CYPHERPUNKS, INTERNET LIBRE & CRYPTOGRAPHIE ASYMÉTRIQUE



+



=



Objectifs

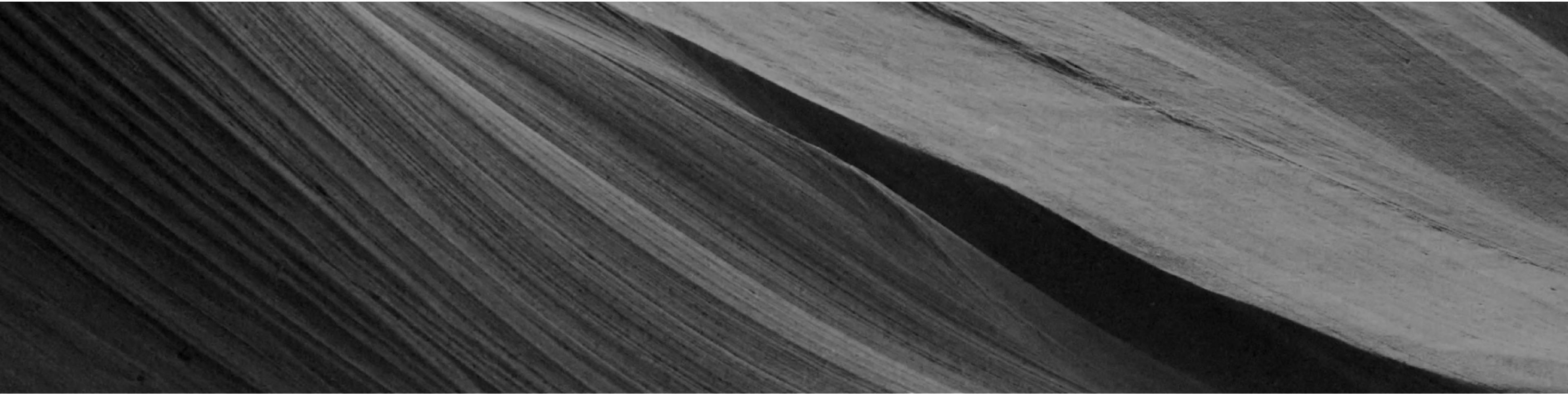
- Internet libre
- Cuperpunks
- Cryptographie

Les concepts

- Internet libre
- Culture libre
- Cypherpunks
- Cryptographie

01

Les inspirateurs





Les inspirateurs

RICHARD STALLMAN

GNU

RMS, rms, la figure tutélaire ([vidéo de 1984](#)).

Prophète du [logiciel libre](#)

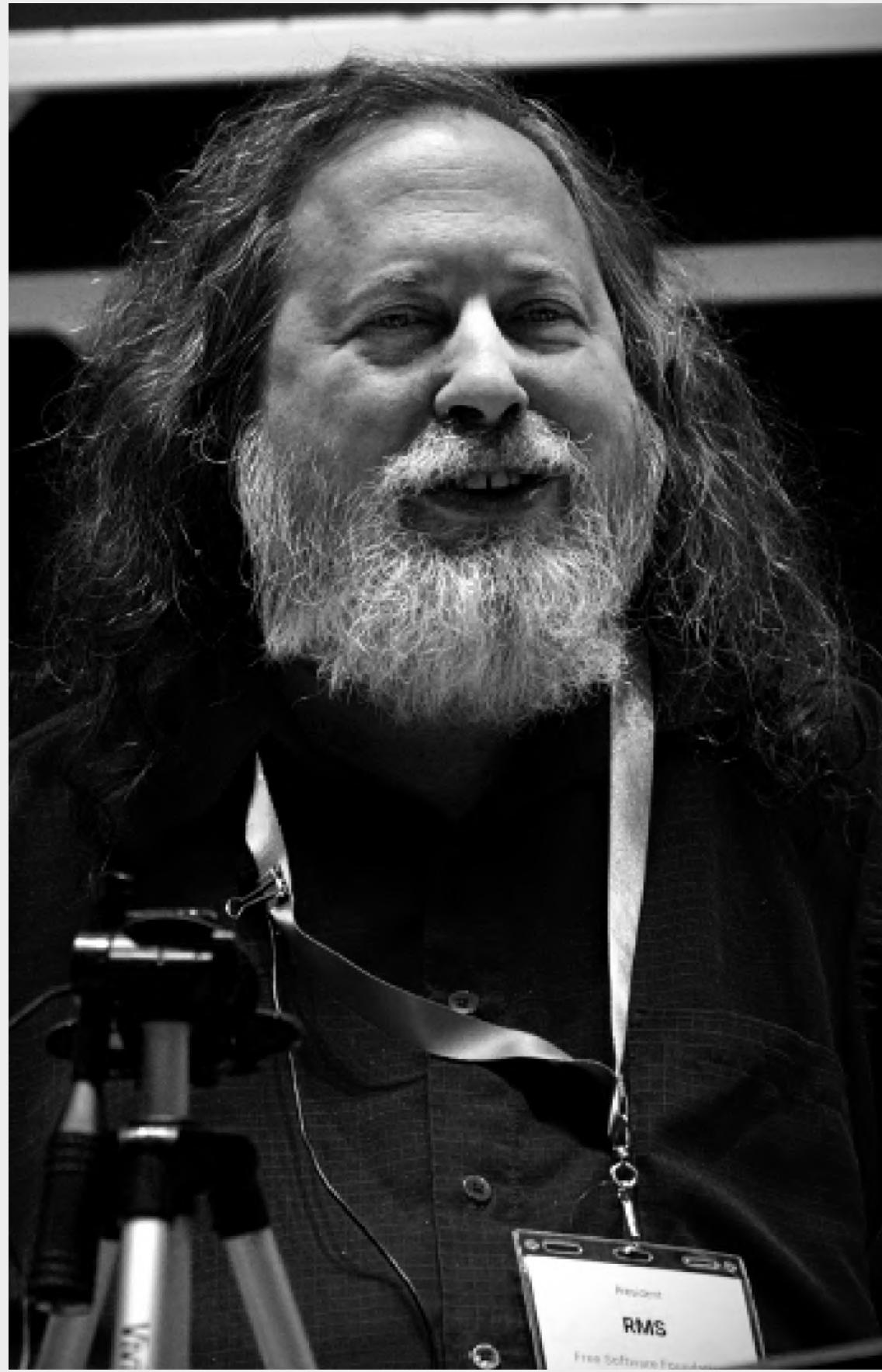
Initiateur du projet [GNU Not Unix](#)

Auteur du [GNU Manifesto](#)

Créateur de la [Licence GNU/GPL](#)

Fondateur de [la Free Software Foundation](#)

Slogan : « Liberté, Egalité, Fraternité » (du logiciel, de l'informatique, de l'humanité)



Les inspirateurs

Genèse du schisme entre informatique centralisé et logiciel libre, France Culture, 5 min, bonne entrée en matière pour novices

TEDx talk d'introduction au logiciel libre et à la libération numérique de nos sociétés, rms, 13 min, vulgarisation aisée et indispensable

Conférence « Intertice 2012 » en français, rms, 1h18, philosophie du logiciel libre, complet et précis, sous licence Creative Commons, évidemment!

Les inspirateurs - Associations informatiques libertaires



Electronic Frontier Foundation
ou EFF



Free Software Foundation
ou FSF

Les inspirateurs - Associations informatiques libertaires

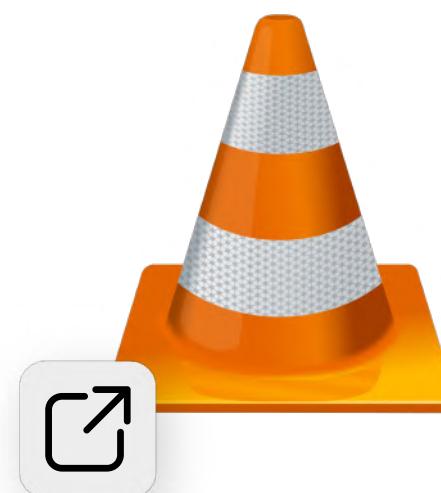
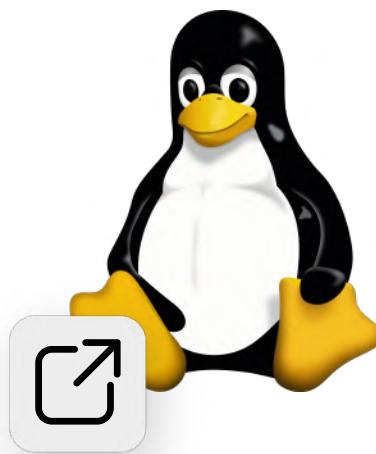


Projet GNU's not Unix ou GNU,
son acronyme récursif



April - Promouvoir et défendre le
logiciel libre

Logiciels libres - quelques exemples célèbres





Les inspirateurs

Lawrence Lessig

Code is law

- Un des plus grand constitutionnalistes au monde,
rédacteur de la constitution géorgienne
- Auteur de l'article référence « Code is law » devenu mantra
- Auteur de Codes et autres lois du cyberspace,
ouvrage de référence



Les inspirateurs

- Initiateur du mouvement de la **Culture Remix** et auteur de l'ouvrage programmatique **Remix**
- Un des leaders du mouvement de la **culture libre**, auteur de **Free Culture**, fondateur de **Creative Commons** et créateur des **Licences Creative Commons**
- [Article biographique](#) de Slate (2017)
- [TEDx Talk sur le mouvement Remix](#), 19 min, didactique et ludique



Les inspirateurs

- TEDx Talk « How Digital Destroyed Democracy », 27min, sur les relations entre media et démocraties à l'heure du numérique
- Conférence TED sur le copyright et les freins légaux à la créativité et au progrès technologique, 19 min, bonne matière concernant la culture libre et l'Internet libre



Les inspirateurs

Aaron Swartz

Wikipedia

- Collaborateur de L. Lessing et chercheur à Harvard à 13 ans
- Cyber activiste, penseur, combattant de la liberté
- Développeur de la licence CC et d'Open Library, bâtisseur et promoteur prolifique de Wikipedia, la plus grande encyclopédie au monde Développeur du format RSS, le web feed le plus utilisé au monde



Les inspirateurs

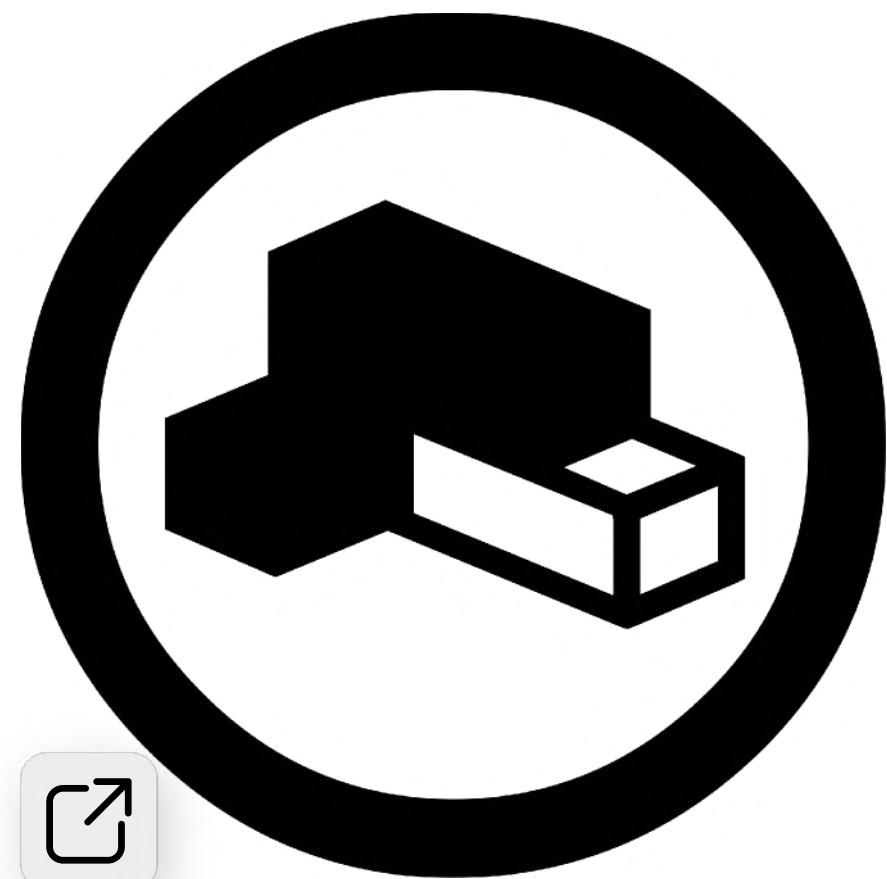
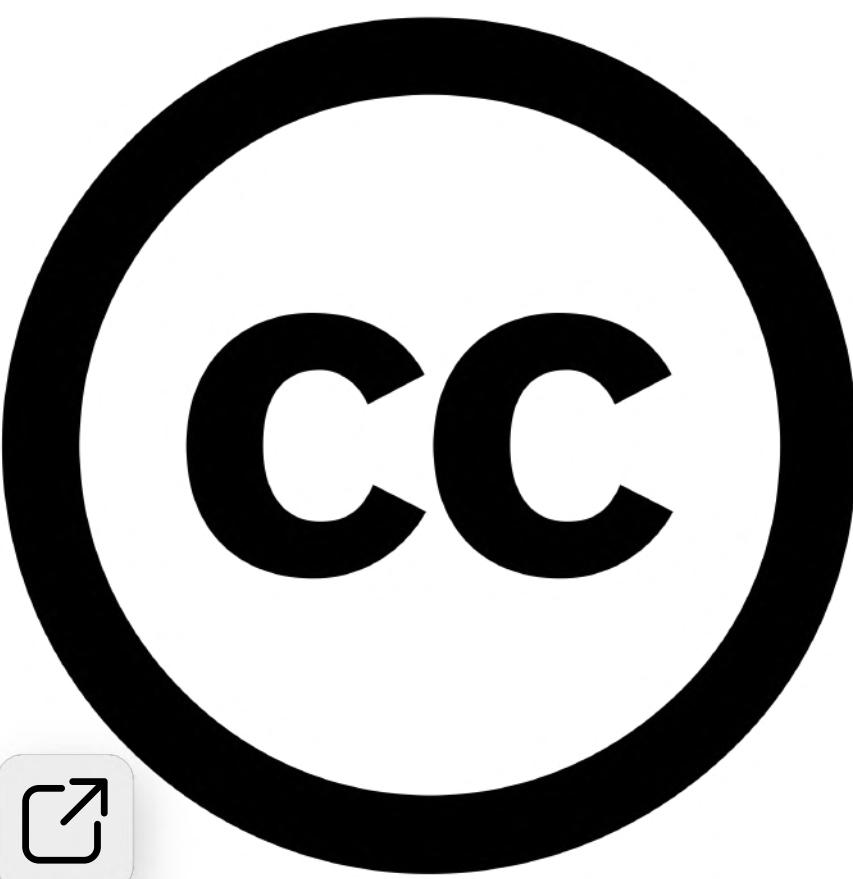
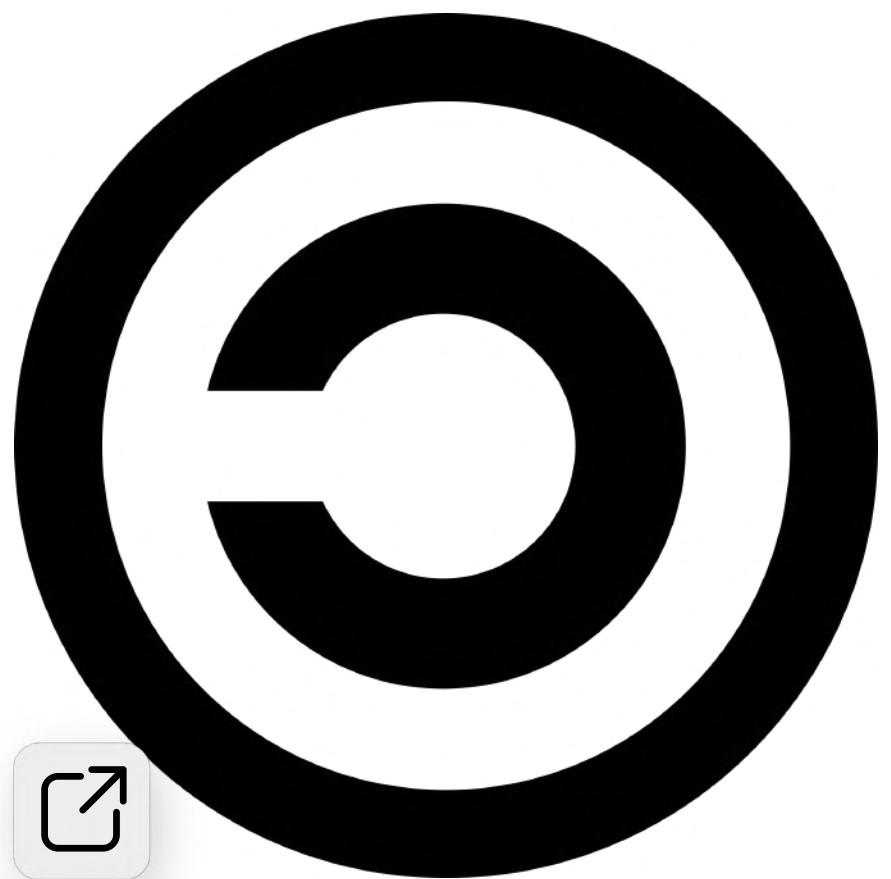
- Principal développeur du projet [Reddit](#)
- Membre du [W3C](#), pour la promotion des standards Internet (développeur du modèle [RDF](#))
- [The Internet's Own Boy](#), film sur la vie d'Aaron Swartz et son combat pour la liberté, Brian Knappenberger, 2014. Libre de droit ([CCL](#)), visionnage indispensable



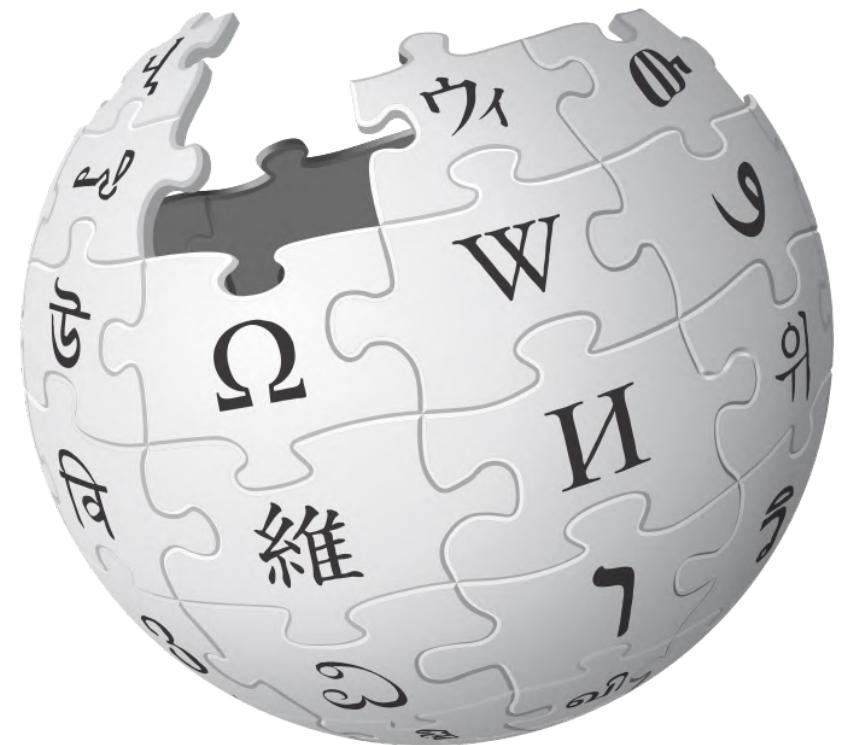
Les inspirateurs

- [Page et podcasts France culture](#), belle synthèse, à découvrir absolument
- [Celui qui pourrait changer le monde](#), œuvre posthume rassemblant ses principales contributions écrites
- [Poursuites américaines](#) concernant l'affaire JSTOR l'ayant poussé au suicide
- [Interview de Lessing à son propos](#), par Telerama

Les inspirateurs - Culture Remix & Culture libre



Les inspirateurs - La culture libre pour le grand public

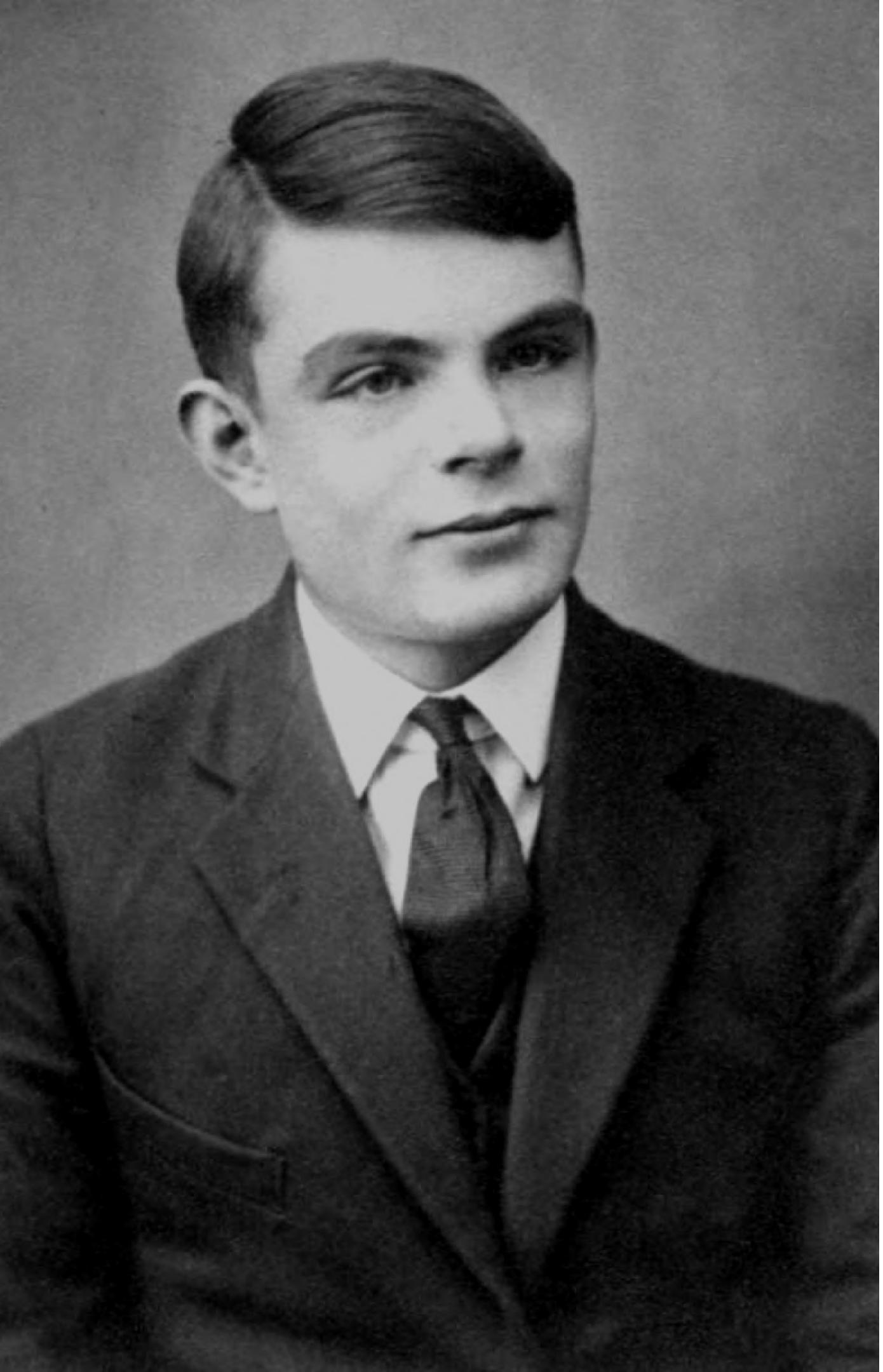


WIKIPÉDIA



L'encyclopédie libre



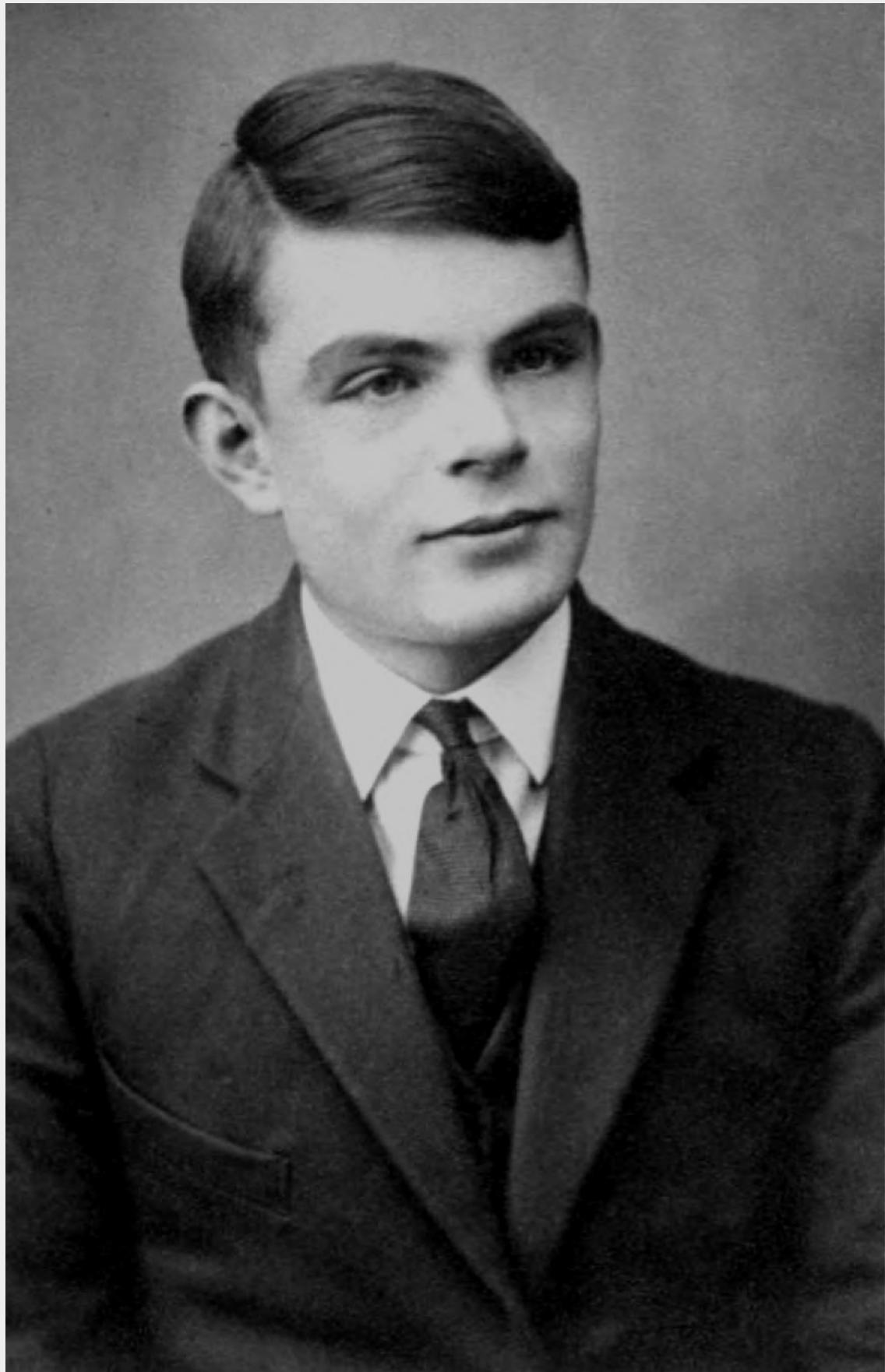


Les inspirateurs

Alan Turing

machine de Turing

- Mathématicien, **cryptologue** (**cryptographe** et **cryptanaliste**) britannique, célèbre pour avoir finalisé la **cryptanalyse des machines Enigma**
- Créeur de la **machine de Turing**, modèle de **calculabilité** et **algorithmique**, qui fonde **l'informatique théorique** et la **philosophie de l'IA**
- Créeur du **test de Turing**, concept fondamental en théorie de l'IA (**jeu de l'imitation à l'aveugle**)



Les inspirateurs

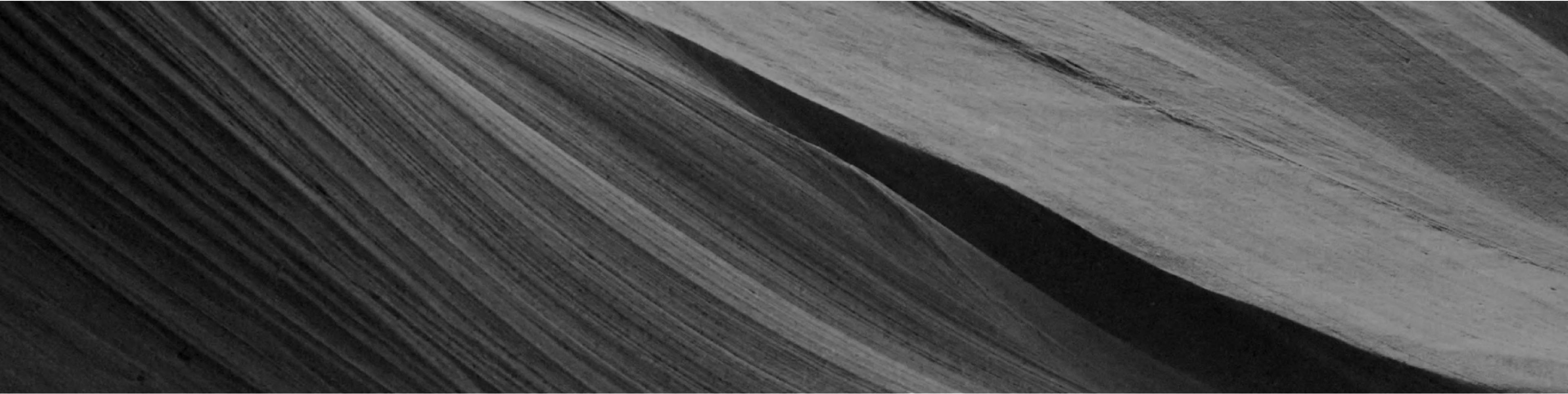
- La résolution du **problème de l'arrêt** et ses recherches sur la **programmation** permettront de créer le premier ordinateur, le **Pilot ACE**
- Travaux sur la morphogenèse ayant contribué à la biologie moléculaire et initié la théorie du chaos

La machine Enigma et la cryptographie assymétrique

- Ce site sous licence MIT (open source) vous permet de tester en direct une multitude de méthodes de chiffrement (symétriques et assymétriques) historiques et modernes, de la machine Enigma à l'algorithme de hachage de Bitcoin (hascash, une méthode d'application du SHA256)
- Une vidéo d'explication simple, claire et juste du fonctionnement d'une machine Enigma
- Une conférence filmée du Pr. David Perry sur le fonctionnement détaillé d'Enigma
- La playlist extraordinairement didactique de Exo7Math concernant la cryptographie

02

Les fondateurs



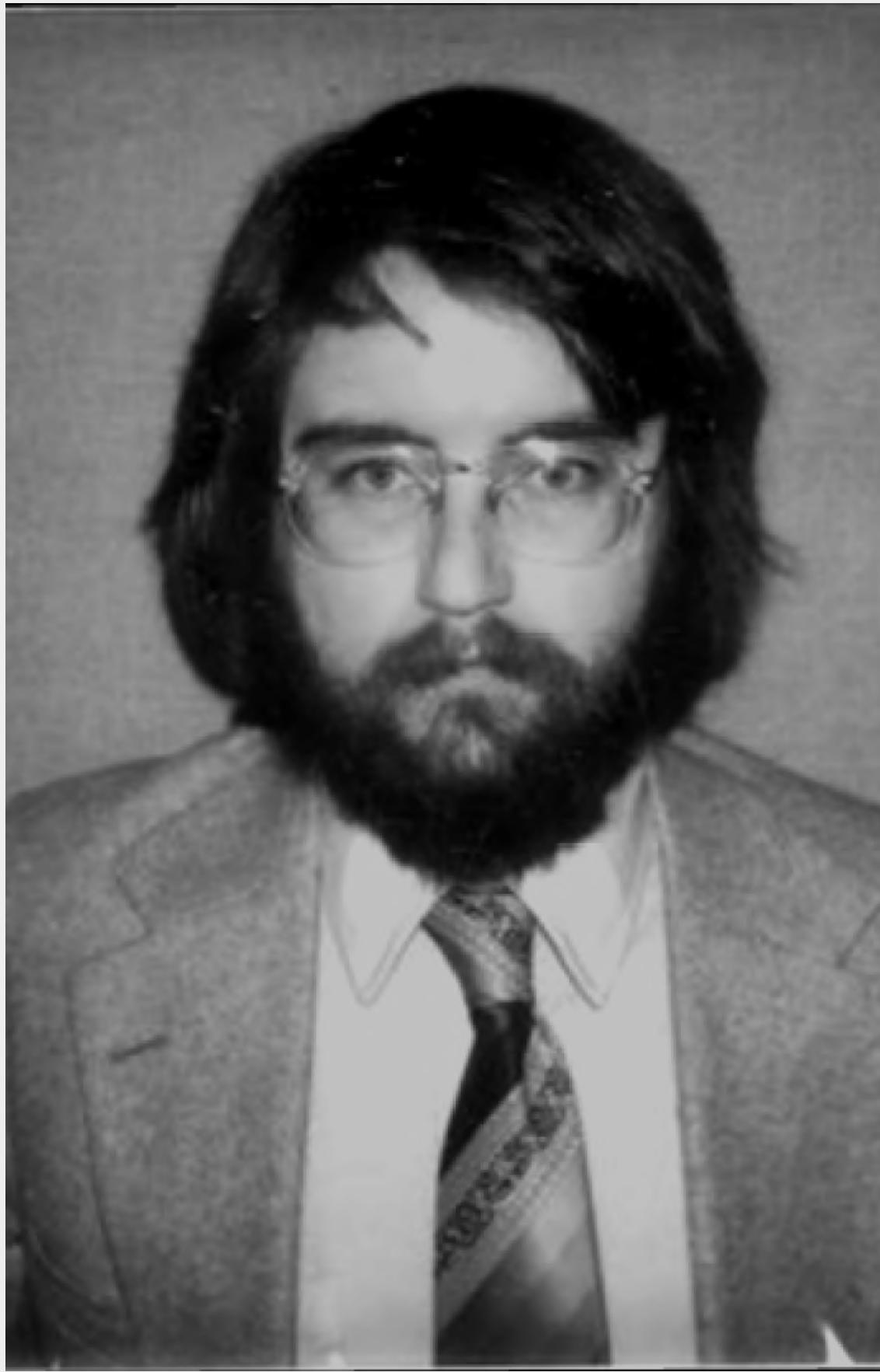


Les fondateurs

Timothy C. May

The Cyphernomicon

- Penseur de la confidentialité des échanges et des données, défenseur de la vie privée
- 贡献者 central à la **liste de diffusion Cypherpunks**, pierre essentielle à la structuration de la communauté
- Auteur du « **Manifeste crypto-anarchiste** », lu au Cypherpunk meeting de septembre 1992



Les fondateurs

- Auteur de **The Cyphernomicon**, conçu comme une FAQ mais faisant office de déclaration programmatique du mouvement cypherpunk
- Conférence « 30 ans de crypto-anarchisme » au Hacker Congress HCPP16, 1h15, exaltant



Les fondateurs

Eric HUGHES

Manifeste cypherpunk

- Auteur du « **Manifeste cypherpunk** » (version originale)
- Administrateur de la liste de diffusion cypherpunk
- Créeur du premier serveur de transmission anonyme
- « Mon objectif principal pour les cypherpunks est d'**amener les gens à défendre leurs confidentialité**, plutôt que de compter sur quelqu'un d'autre pour le fournir. » Eric Hughes – Cypherpunk Mailing List, 23 mars 1993

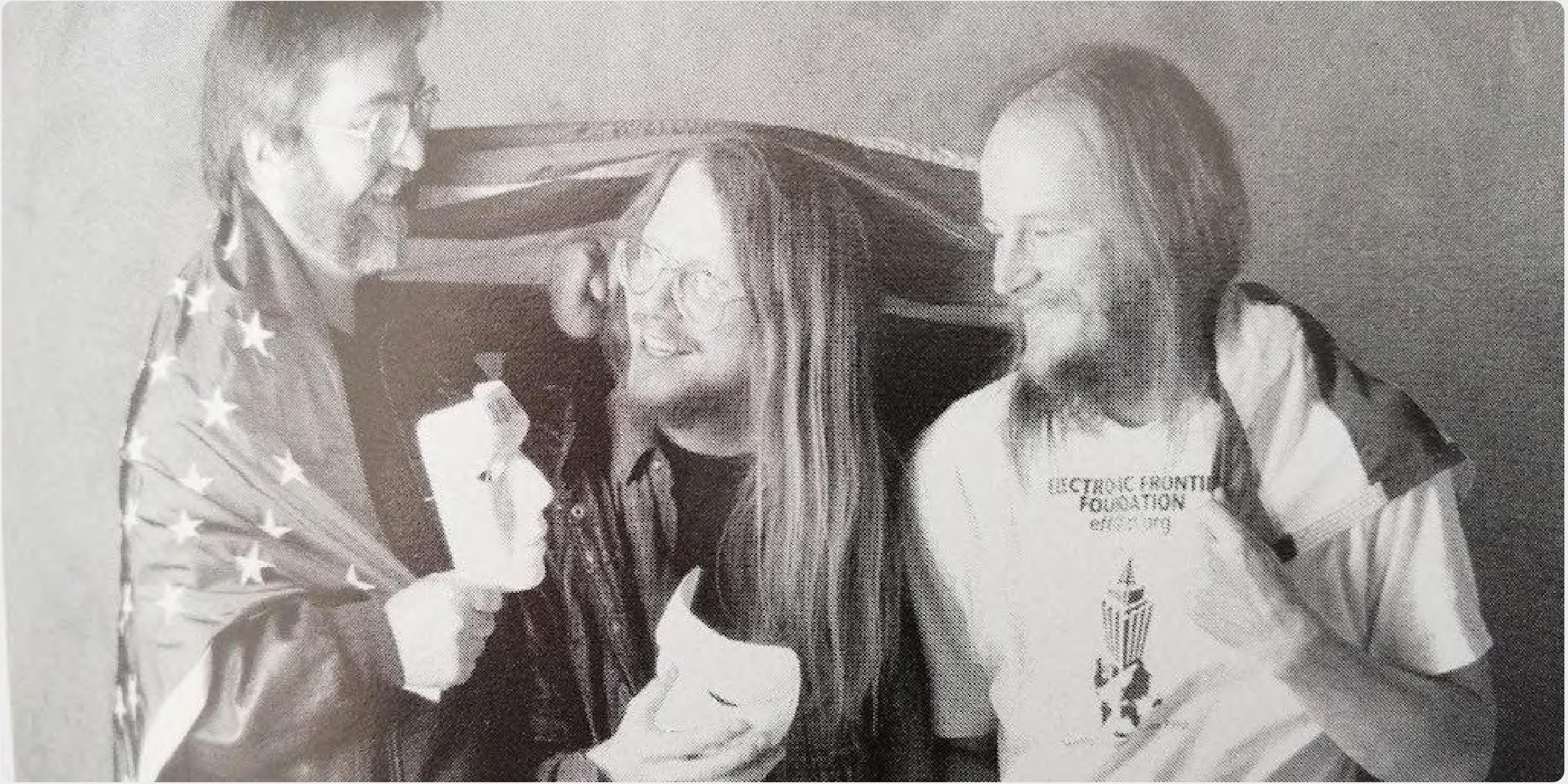


Les fondateurs

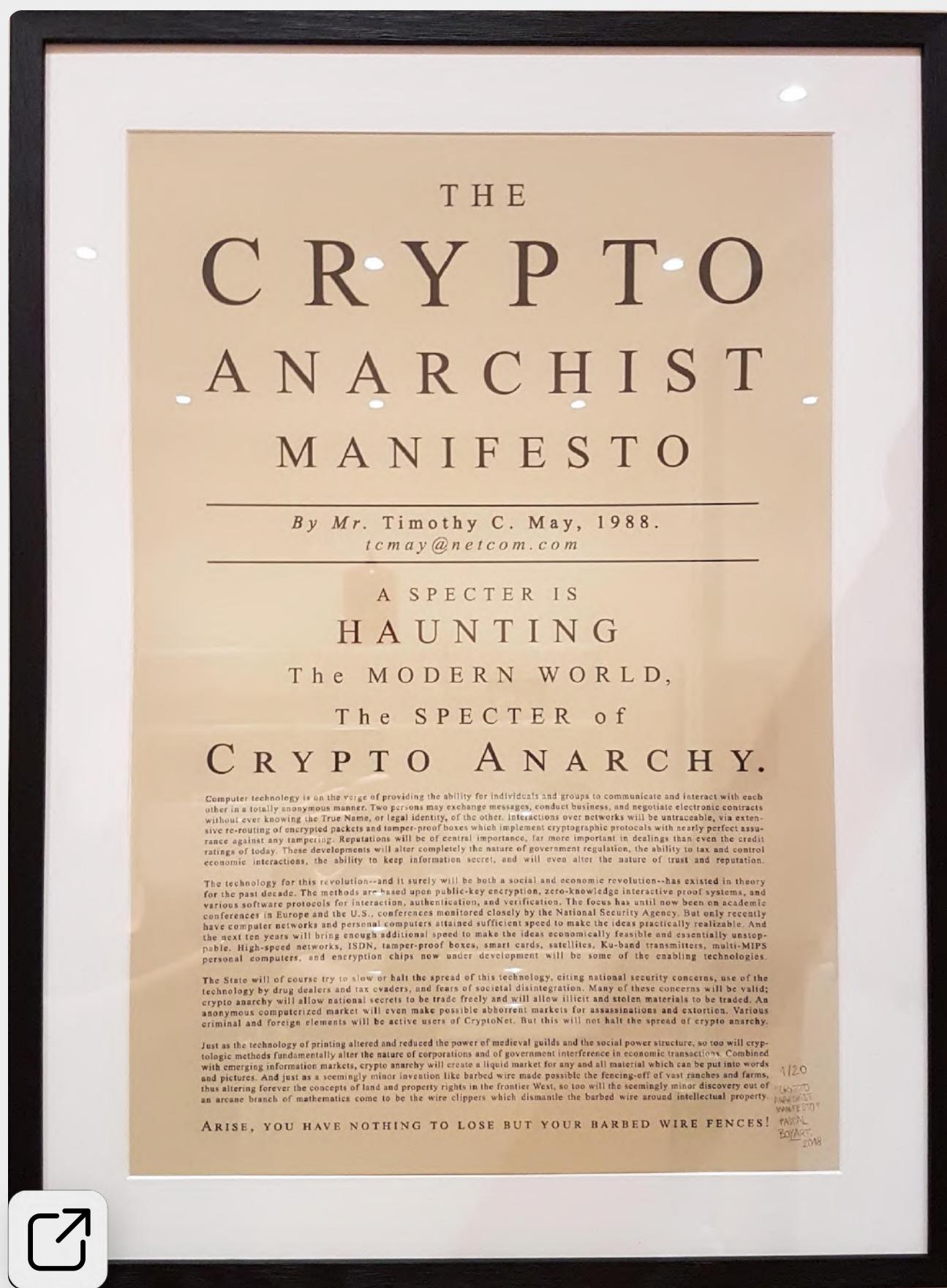
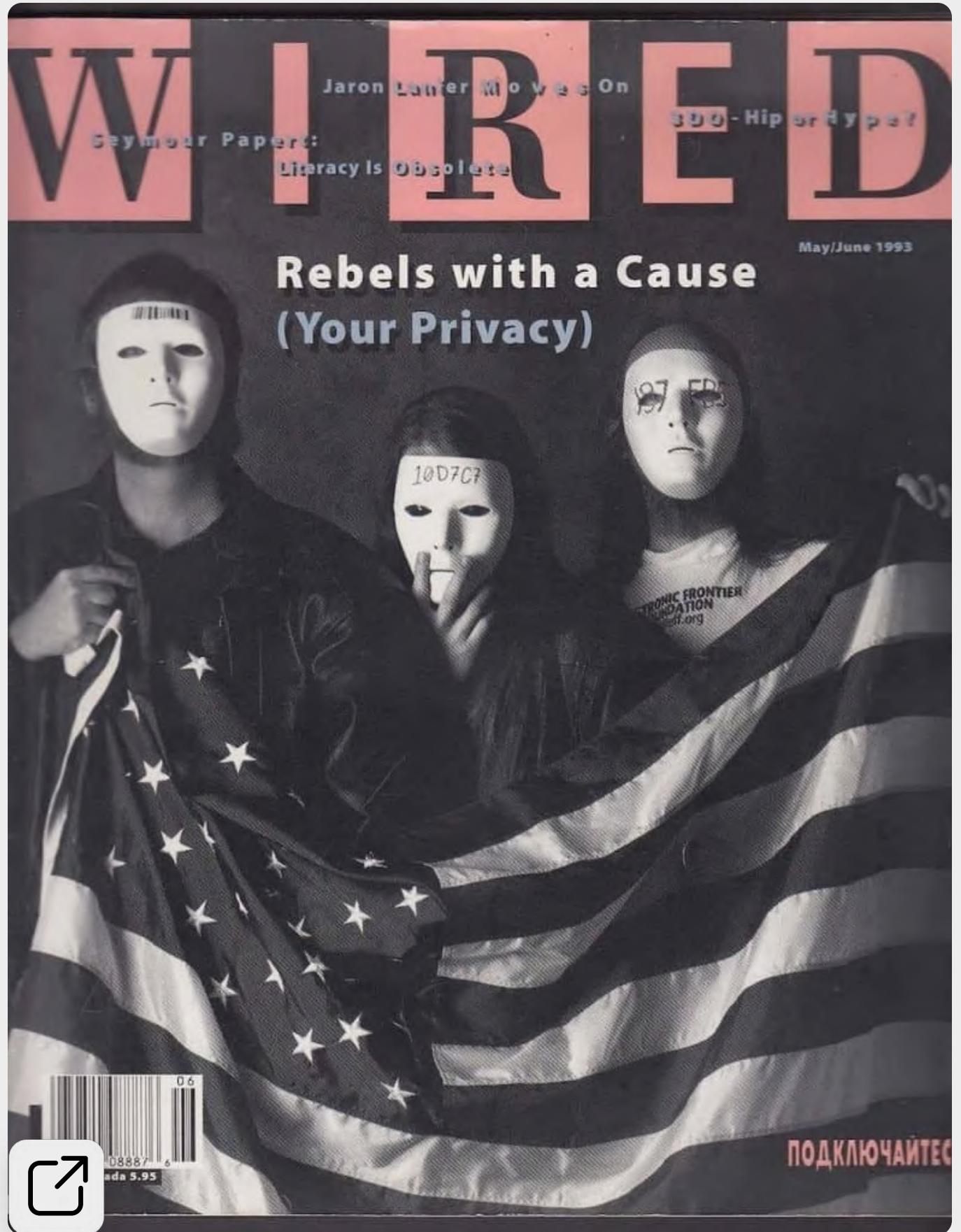
John GUILMORE

Usenet

- Membre fondateur de l'Electronic Frontier Foundation et de la Cypherpunk mailing list
- Contributeur Usenet, système précurseur d'Internet (forums organisés en réseau)
- Contributeur à des réalisations phares du projet GNU, notamment GNU Debugger, GNURadio, Gnash et GNUTar
- Coauteur du protocole Bootstrap pour attribution d'IP
- Promoteur du chiffrement généralisé des communications Internet (Ipsec et OE)



ELECTRONIC FRONTIER
FOUNDATION
eff.org



La révolution cypherpunk

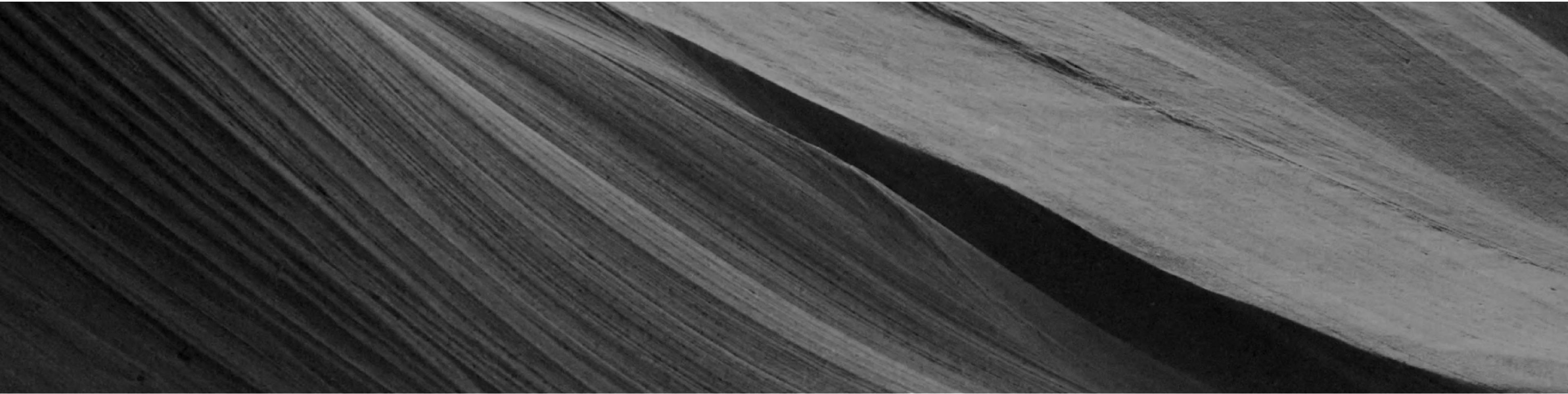
- Document original, **The cypherpunk revolution**, par Thomas Rid, reprenant l'intégralité de l'histoire de ce mouvement computationnel et anarchiste, cryptographique et libertaire.
- Article original de Steven Levy, **Crypto Rebels** pour *Wired* sur le mouvement cypherpunk, datant du 2 janvier 1993 mais d'une actualité saisissante
- Archive contenant l'intégralité des contributions, à la mailing list cypherpunk, permettant émulation et échanges d'idées entre pairs, garantissant la vitalité de la communauté. Document exceptionnel.



Street Art, Banksy. Crédits photo : Reuters

03

Les bâtisseurs





Les bâtisseurs

David CHAUM

Wikileaks

Sa dissertation « Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups »

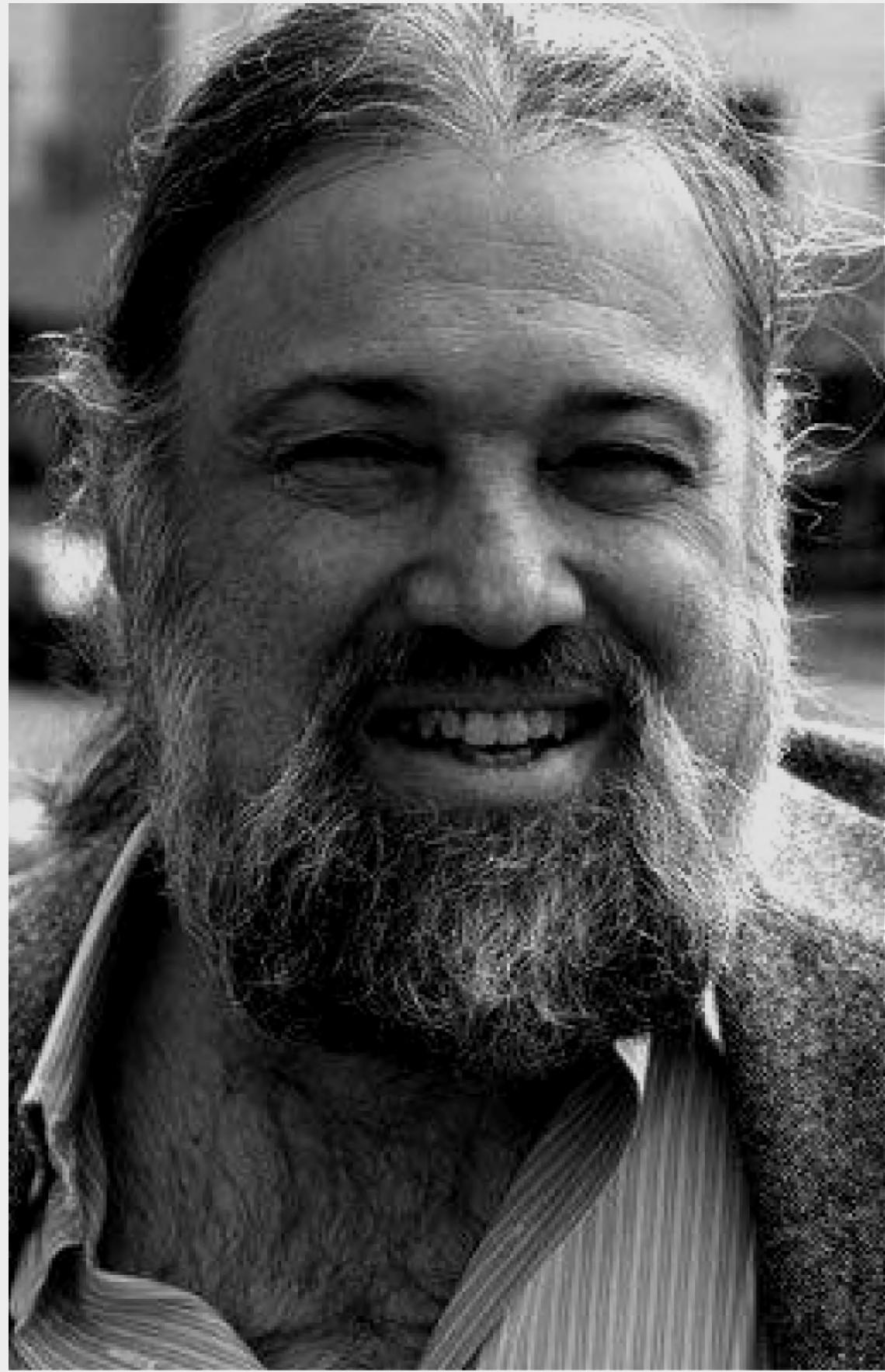
réalisée en 1982 à Berkeley peut être vue comme la
première théorisation d'un protocole blockchain.

L'intégralité des éléments constitutifs de Bitcoin y sont
présentés et décrits, à l'exception du mécanisme de
preuve de travail



Les bâtisseurs

Son papier de 1983 « *Blind signatures for untraceable payments* » en fait l'**inventeur du concept de monnaie digitale** ainsi que du concept de **signature aveugle**, fondamental pour établir une monnaie électronique (certification de la signature sans divulgation du message)



Les bâtisseurs

- Créeateur en 1981 du concept de Mix Network, une chaîne de serveurs proxys, prémissse du futur réseau Tor
- Inventeur, en 1989 du concept de signature indéniable, lui permettant de proposer un protocole cryptographique à divulgation nulle de connaissance
- Inventeur, en 1991, du concept de signature de groupe (signature sécurisée d'un utilisateur au nom d'un groupe avec préservation de son anonymat)
- Inventeur du système Ecash en 1983 et fondateur de DigiCash, la première monnaie électronique, lancée en 1990, victime de son avant-gardisme

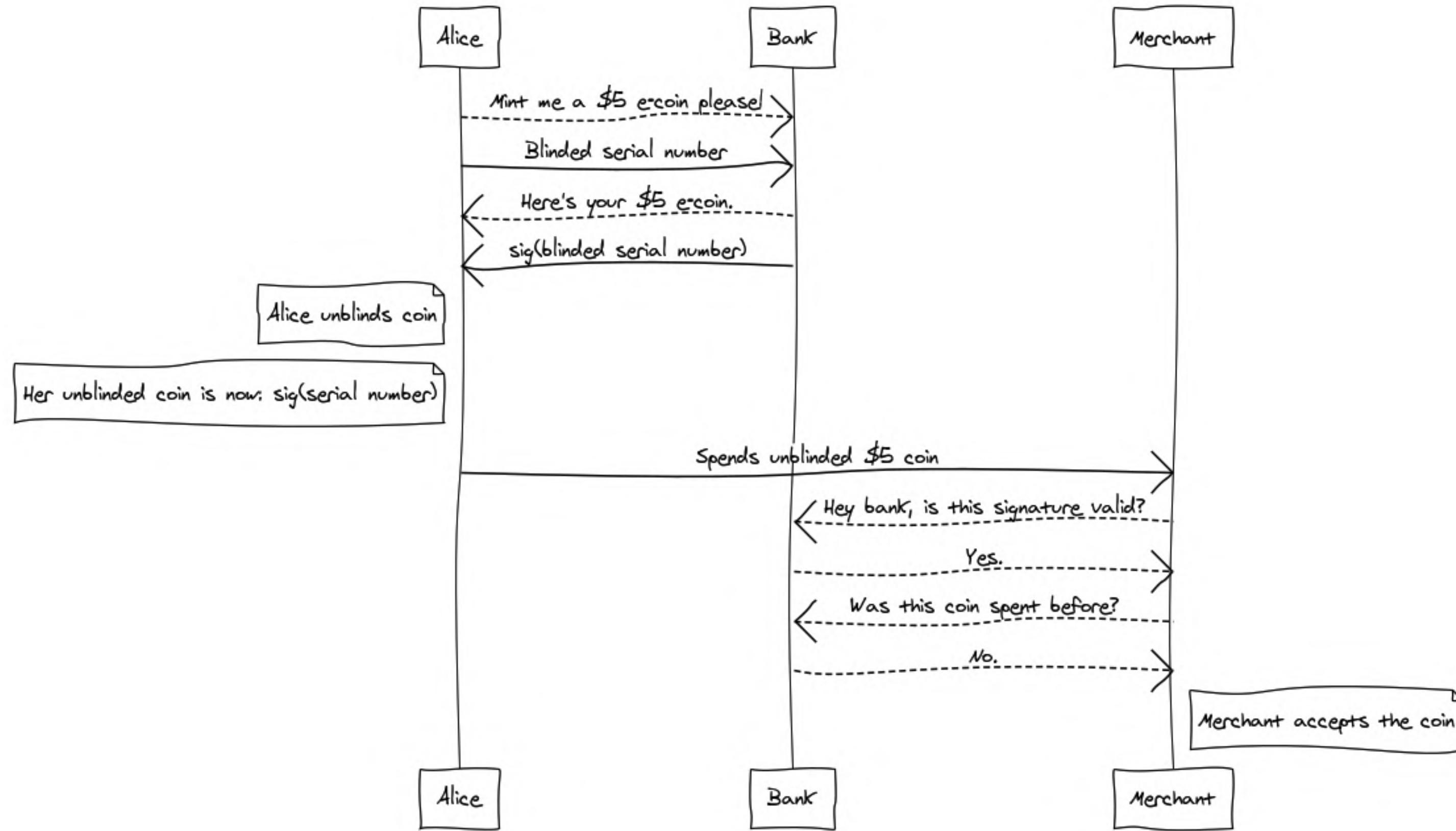


Diagramme du protocole Ecash, 1ere itération d'une monnaie électronique



Les batisseurs

Adam BACK Hashcash

Créateur en 1997 de **hashcash**, un système de hachage anti-spam (anti-Dos), résolvant une problématique fondamentale des monnaies électroniques et constituant l'algorithme de consensus de Bitcoin



Les batisseurs

Adam Back est le PDG de Blockstream, une des principales compagnies travaillant au développement du protocole Bitcoin (pourvoyeur de fonds pour développeurs tels Bitcoin Core) ainsi qu'à son amélioration (participation au réseau Lightning et gestion de la sidechain pro-exchanges Liquid)

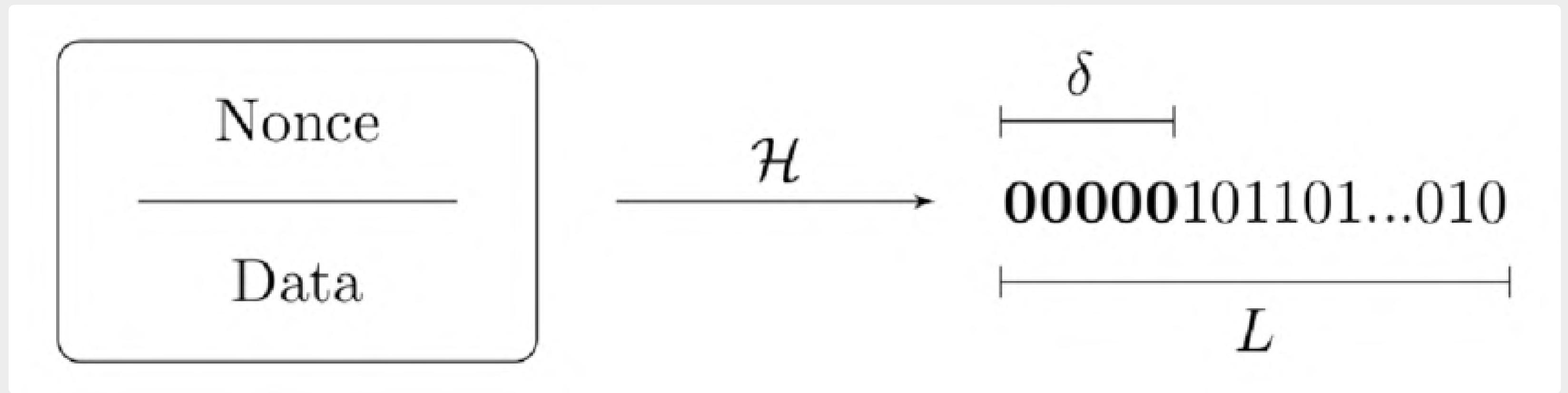


Schéma basique de fonctionnement du hashcash, proposé par Adam Back



Les batisseurs

Wei DAI

B-money

- Créeateur en 1995 de la **librairie Crypto++** (en C++) sous licence libre et open source, largement utilisée pour les travaux académiques et de recherche
- Créeateur en 2007 de **VMAC**, un algorithme de code d'authentification de message (MAC) basé sur une méthode de **chiffrement par bloc**



Les batisseurs

- En cryptographie asymétrique, le chiffrement par bloc, alternative au chiffrement par flot, ouvre la voie à une monnaie électronique sécurisée par nonce : Bitcoin n'est pas loin...
- Fondateur en 1998 de B-money, « une monnaie impossible à réguler »



Les batisseurs

B-money améliore les précédentes propositions de monnaie électronique, en intégrant le principe du **hashcash** théorisé par Back : pour fonctionner, B-money nécessite un calcul computationnel important, c'est la naissance de la **preuve de travail** (Proof Of Work, PoW), principal méthode de sécurisation des blockchains existantes, appelée **méthode de consensus**



Les batisseurs

- B-money consacre également le principe de l'**horodatage des transactions** en **P2P**, ainsi que l'application du concept de **signature digitale asymétrique**
- Wei Dai et Adam Back sont les deux premières personnes que Satoshi Nakamoto contacte en 2008 / B-monney est explicitement cité dans le **whitepaper de Bitcoin**
- Site personnel de Wei Dai et whitepaper de « B-money, an anonymous, distributed electronic cash system »

'In a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary.'

Wei-Dai, B-Money



Les bâtisseurs

Nick SZABO BitGold

- Nick Szabo – créateur du principe des smart contract, dont l'existence, peu favorisée par Bitcoin, a été popularisée par la blockchain Ethereum
- Auteur de la proposition BitGold, jamais implémentée, faute de fonds, mais préfigurant Bitcoin



Les batisseurs

- BitGold introduit un élément théorique fondamental pour le succès futur d'une monnaie numérique décentralisée : la rareté, artificiellement créée mais certainement garantie, grâce au concept de puzzle cryptographique, soit la résolution de la preuve de travail (PoW)
- BitGold incorpore des éléments fondamentaux d'une blockchain : PoW, horodatage, cryptographie à clef publique



Les batisseurs

- BitGold parvient à juguler le problème théorique de double dépense, raison d'être des intermédiaires monétaires et financiers certificateurs
- Pour se faire, son modèle est basé sur la résolution du problème des généraux byzantins, lui permettant ainsi de juguler le risque d'attaque de type 51, permettant théoriquement de réaliser des double dépenses



Les bâtisseurs

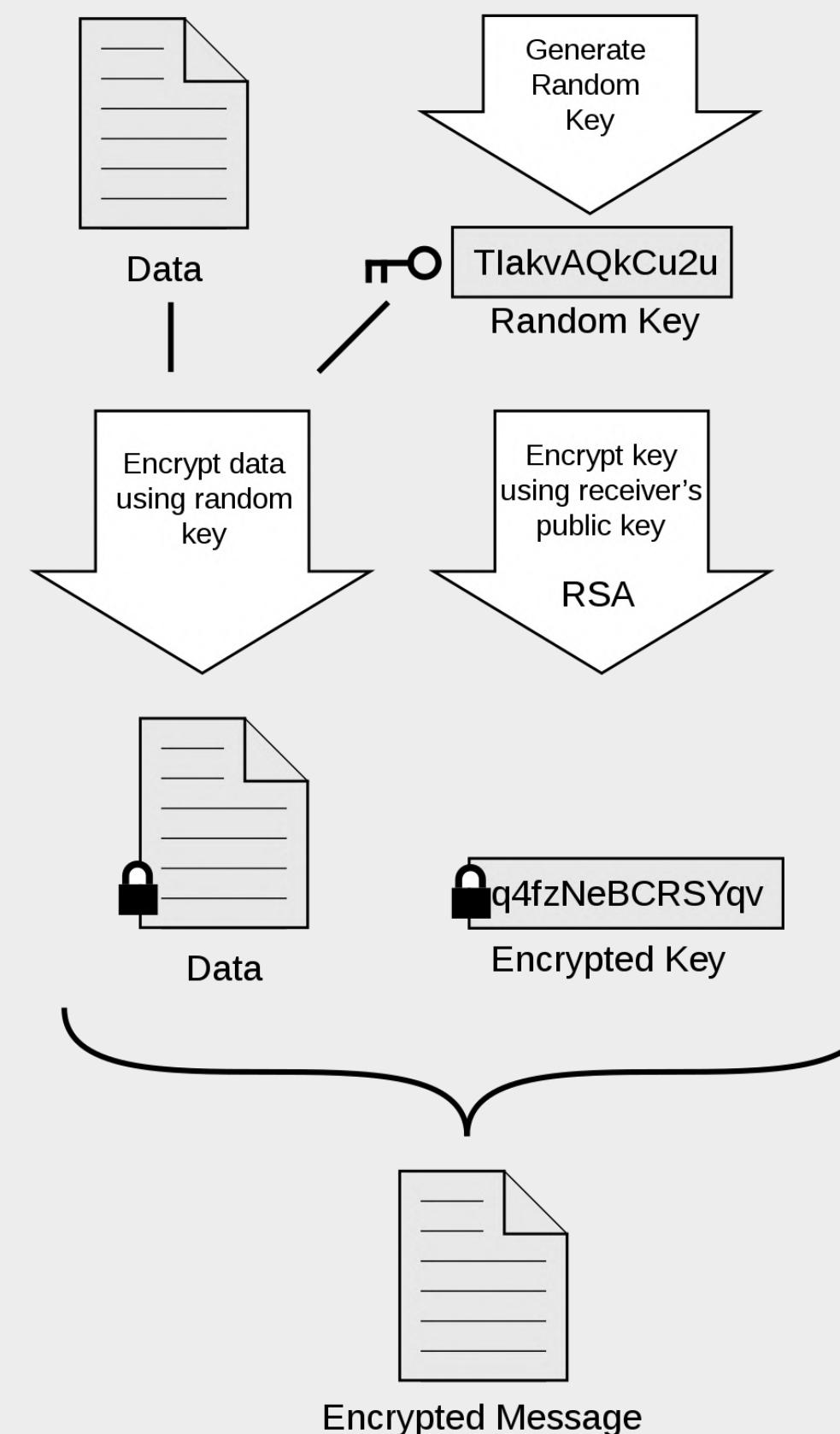
Hal FINNEY

PGP

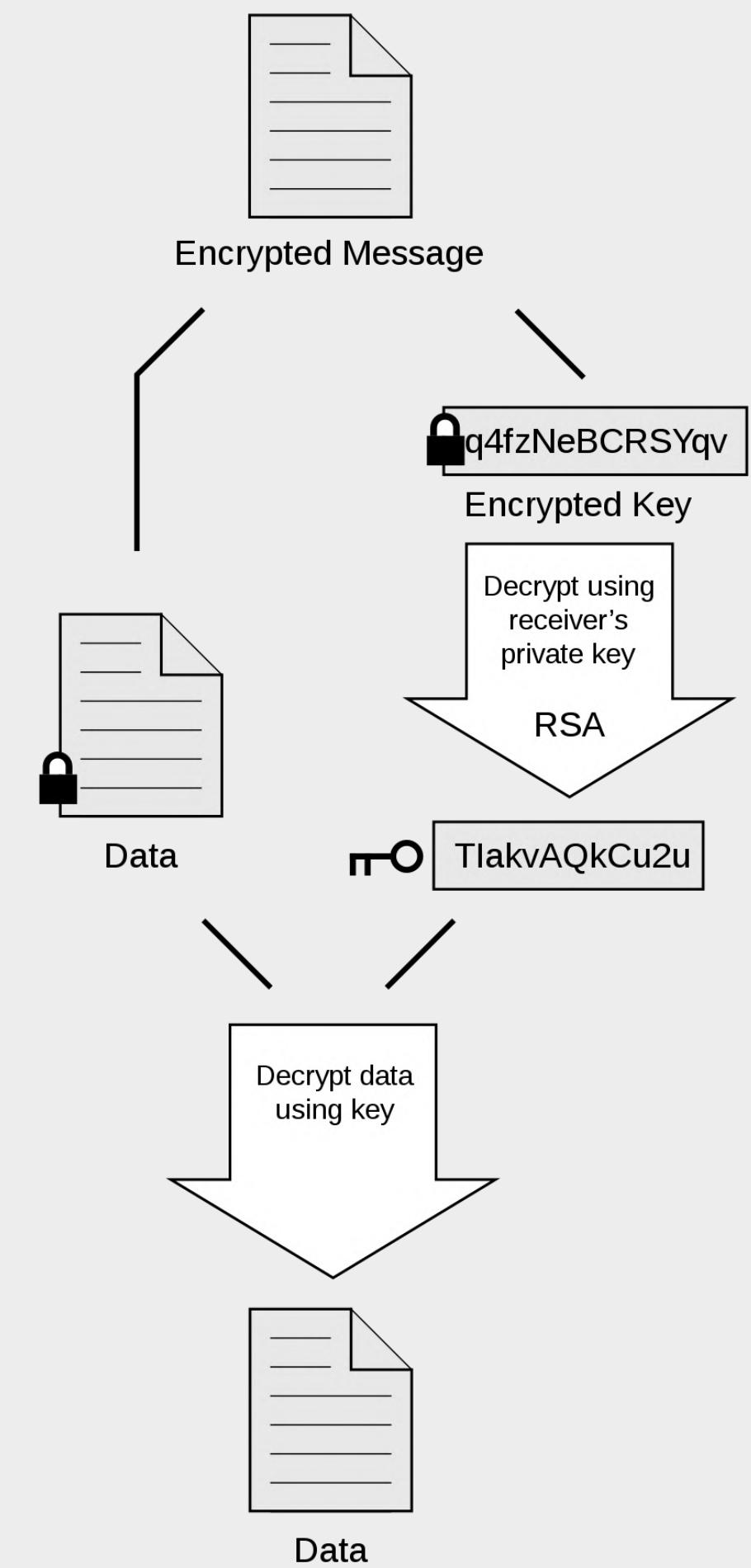
- Ancien développeur de jeux vidéos
- Développeur du programme PGP (Pretty Good Privacy), logiciel de chiffrement des communications, avec Phil Zimmermann, en 1991
- 贡献者 de la première heure au protocole Bitcoin, avec Wei Dai et Nick Szabo
- Destinataire de la première transaction Bitcoin, par Satoshi Nakamoto, en 2009

Le protocole PGP

Encrypt



Decrypt



« When Satoshi announced the first release of the software, I grabbed it right away. I think I was the first person besides Satoshi to run bitcoin. I mined block 70-something, and I was the recipient of the first bitcoin transaction, when Satoshi sent ten coins to me as a test. I carried on an email conversation with Satoshi over the next few days, mostly me reporting bugs and him fixing them. Today, Satoshi's true identity has become a mystery. But at the time, I thought I was dealing with a young man of Japanese ancestry who was very smart and sincere. I've had the good fortune to know many brilliant people over the course of my life, so I recognize the signs. After a few days, bitcoin was running pretty stably, so I left it running. Those were the days when difficulty was 1, and you could find blocks with a CPU, not even a GPU. I mined several blocks over the next days. But I turned it off because it made my computer run hot, and the fan noise bothered me. In retrospect, I wish I had kept it up longer, but on the other hand I was extraordinarily lucky to be there at the beginning. It's one of those glass half full half empty things.

The next I heard of Bitcoin was late 2010, when I was surprised to find that it was not only still going, bitcoins actually had monetary value. I dusted off my old wallet, and was relieved to discover that my bitcoins were still there. As the price climbed up to real money, I transferred the coins into an offline wallet, where hopefully they'll be worth something to my heirs. »

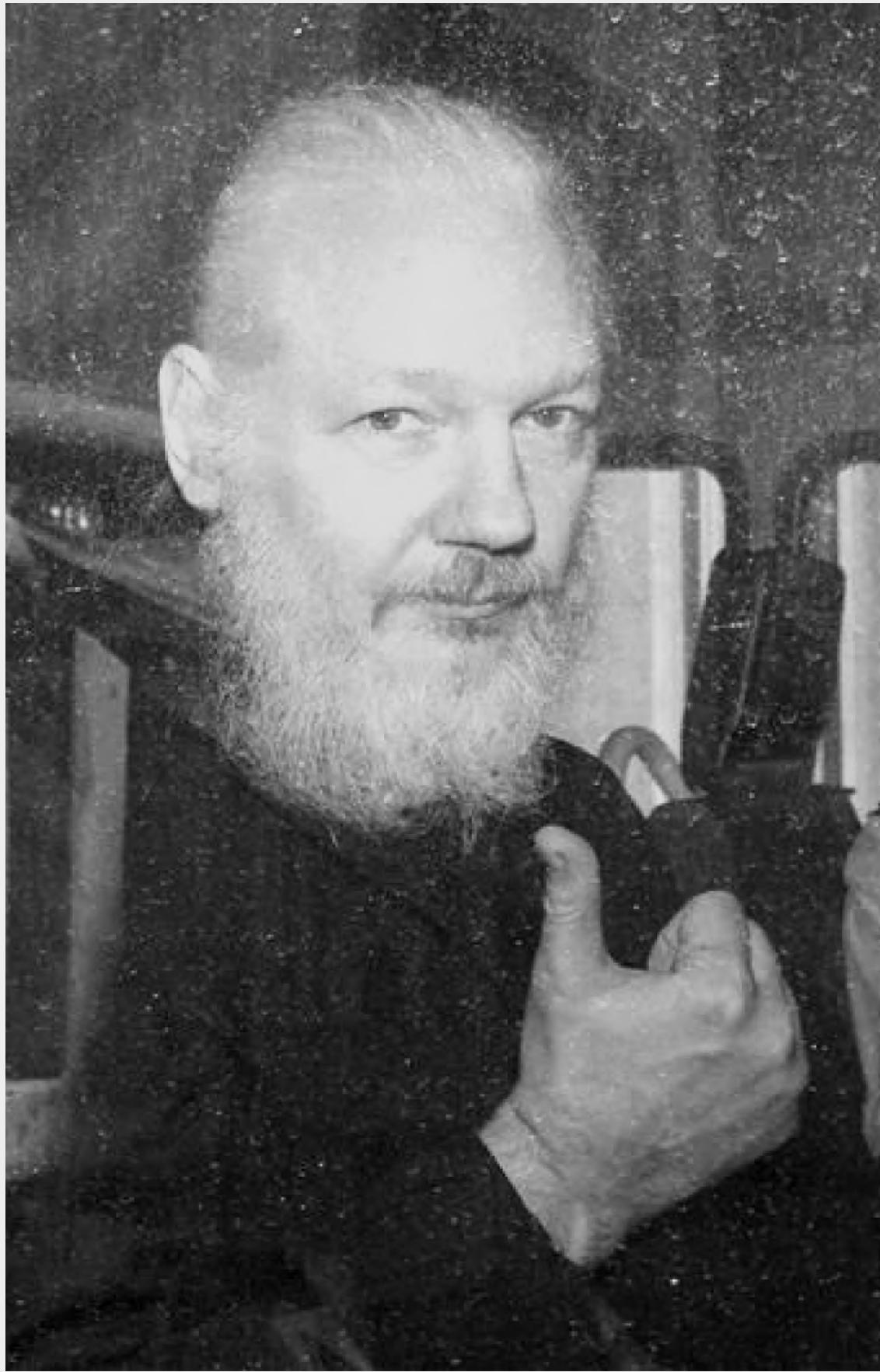
Hal FINNEY, 2013, quelques mois avant sa mort, sur le forum Bitcointalk



Les batisseurs

Julian Assange Wikileaks

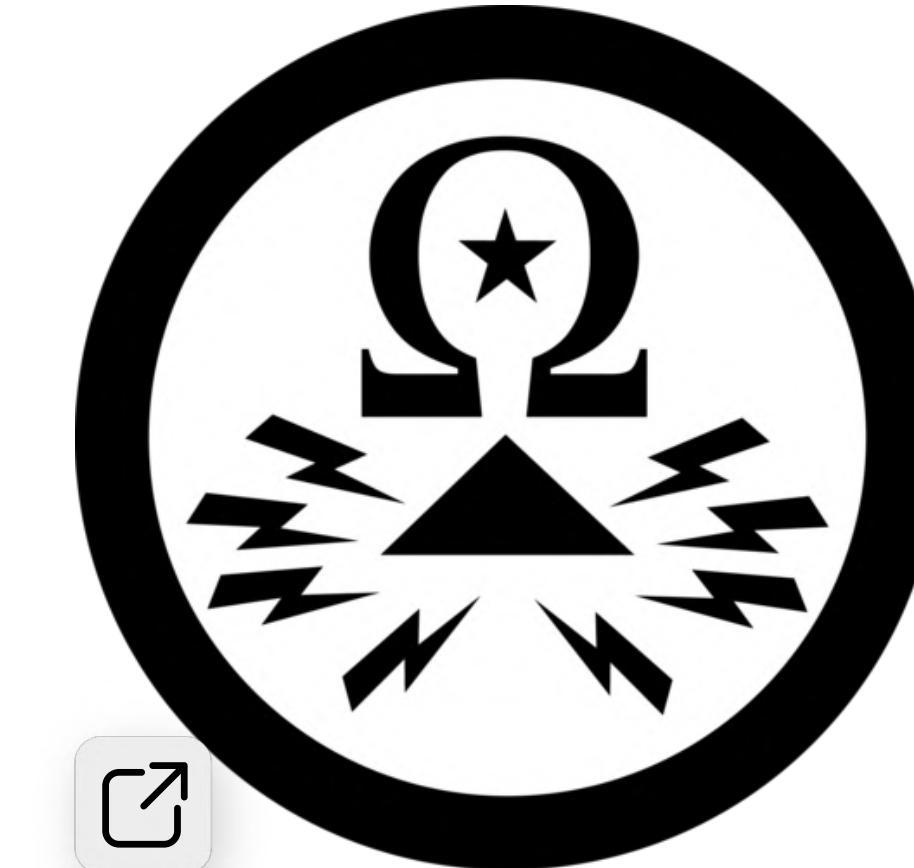
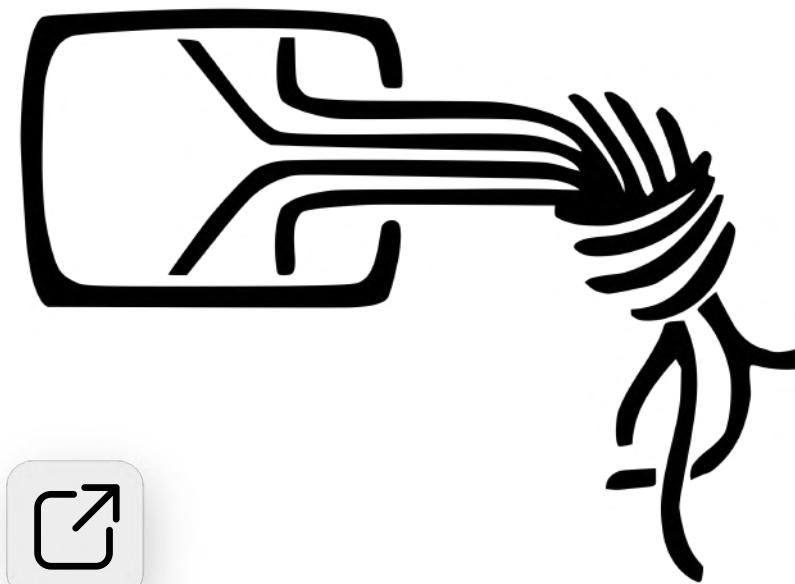
- Cyber activiste et hacktiviste
- Cryptographe, cypherpunk et crypto-anarchiste,
- Spécialiste des **tests d'intrusion**, ancien célèbre **white hat** surnommé Mendax
- Fondateur de Wikileaks, lanceur d'alertes



Les batisseurs

Prisonnier politique : enfermé illégalement à la prison de haute sécurité Belmarsh, au Royaume-Uni, tortures systématiques, tentative d'assassinat par la CIA en 2017 Documentaire de LCP de 2021, Julian Assange, le prix de la vérité

Cybermilitantisme et hacktivisme



A cypherpunk discussion : [Partie 1](#) et [Partie 2](#)



Jeremie Zimmermann



Andy Muller Maguhn



Jacob Appelbaum



Julian Assange





A LA DÉCOUVERTE DES BLOCKCHAINS PUBLIQUES

Consultant Blockchain

A suivre...

Bitcoin

Consultant Blockchain

Alyra - Bastien Ebalard