

The History & Philosophy Of Cypherpunk

Harry Halpin

CEO, Nym

Max Hampshire

DevRel, Nym



Never bend the knee: No Authority but Yourself



Ryan Selkis (d/acc) 🇺🇸 🐦 @twobitidiot · 43m
Replying to @AdrianoFeria and @groupreadaccess
Are you a citizen or just a green card holder?

1 73

AdrianoFeria.eth 🏠 🛡️ 🐦 @AdrianoFeria
Replying to @twobitidiot and @groupreadaccess
I've been a green card holder for more than a decade and am about to initiate the process of becoming a citizen. What practical difference does that make in the context of this conversation?

18:44 · 17 Jul 24 · 82 Views

3 Likes

Related posts

Ryan Selkis (d/acc) 🇺🇸 🐦 @twobitidiot · 7m
Replying to @AdrianoFeria and @groupreadaccess
I hope we send you back. That's why I was asking. Sorry.

Pierre Proudhon

Inventor of term “anarchism”

Mutualism

Time-chits

“Labour Vouchers” and debate
with Marx

The Principle of Federation
(1863)



The Socialist Calculation Debate

The origin of Libertarianism
(Hayek, Van Mises)

Centralized vs. Decentralized
planning w/i or without money?

Otto van Neurath (socialist):
Money does not capture
externalities and well-being of
population.

Economic Calculation in the Socialist Commonwealth

by
Ludwig von Mises

Secrecy and the State

See Halpin's "The Philosophy of Secrecy" at *Histocrypt 2024* for pre-computer privacy and cryptographic history from Sumer to Turing:

<https://dspace.ut.ee/items/270e5628-d324-4c5c-a433-a7041137bd04>

"The Adversary: The Philosophy of Cryptography" (forthcoming in *Journal of Cybersecurity*) for detailed history and philosophy of cryptography.

Thesis: The spread of cryptographic techniques such as public-key cryptography outside of the state creates an inevitable schism as non-state actors can build forms of sovereignty via secrecy at the expense of the nation-state.

A historic shift the focus of sovereignty to individuals that wish to escape the transparency that the state enforces on their own population, creating new forms of sovereignty, which leads to the inexorable need for nation-states to break the cryptographic techniques used by individuals (including those in their own population) with the same concern once reserved for competing nation-states.

Diffie-Hellman (1976)

Whitfield Diffie &
Martin Hellman put
public key
cryptography into the
public domain

Create shared secret
key over non
confidential channel

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

David Chaum (1979/1981)

Invents mix-nets

Anonymous untraceable
communication networks

Protect data & metadata

Technical Note
Programming Techniques
and Data Structures

R. Rivest
Editor

Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms

David L. Chaum
University of California, Berkeley

A technique based on public key cryptography is presented that allows an electronic mail system to hide who a participant communicates with as well as the content of the communication—in spite of an unsecured underlying telecommunication system. The technique does not require a universally trusted authority. One correspondent can remain anonymous to a second, while allowing the second to respond via an untraceable return address.

The technique can also be used to form rosters of untraceable digital pseudonyms from selected applications. Applicants retain the exclusive ability to form digital signatures corresponding to their pseudonyms. Elections in which any interested party can verify that the ballots have been properly counted are possible if anonymously mailed ballots are signed with pseudonyms from a roster of registered voters. Another use allows an

of message content for thousands of years [3]. Recently, some new solutions to the “key distribution problem” (the problem of providing each communicant with a secret key) have been suggested [2, 4], under the name of public key cryptography. Another cryptographic problem, “the traffic analysis problem” (the problem of keeping confidential who converses with whom, and when they converse), will become increasingly important with the growth of electronic mail. This paper presents a solution to the traffic analysis problem that is based on public key cryptography. Baran has solved the traffic analysis problem for networks [1], but requires each participant to trust a common authority. In contrast, systems based on the solution advanced here can be compromised only by subversion or conspiracy of all of a set of authorities. Ideally, each participant is an authority.

The following two sections introduce the notation and assumptions. Then the basic concepts are introduced for some special cases involving a series of one or more authorities. The final section covers general purpose mail networks.

Notation

Someone becomes a user of a public key cryptosystem (like that of Rivest, Shamir, and Adleman [5]) by creating a pair of keys K and K^{-1} from a suitable randomly generated seed. The public key K is made known to the other users or anyone else who cares to know it; the private key K^{-1} is never divulged. The encryption of X with key K will be denoted $K(X)$, and is just the image of X under the mapping implemented by the crypto-

David Chaum (1985)

Anonymous credentials: defend against “dossier society”:

“Computerisation is robbing individuals of the ability to monitor and control the ways information about them is used”

Mixnets: communicate privately

Credentials: transact privately

ARTICLES

SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE

The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.

DAVID CHAUM

Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate. The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a “chilling effect,” causing people to alter their observable activities. As computerization becomes more pervasive, the potential for these problems will grow dramatically.

On the other hand, organizations are vulnerable to abuses by individuals. Everyone pays indirectly when cash, checks, consumer credit, insurance, and social services are misused. The obvious solution for organizations is to devise more pervasive, efficient, and interlinked computerized record-keeping systems

for machine-readable national identity documents are gaining momentum. But organizations already use such essentially identifying data as name, date, and place of birth or name and address to match or link their records on individuals with those maintained by other organizations.

With the new approach, an individual uses a different account number or “digital pseudonym” with each organization. Individuals will create all such pseudonyms by a special random process. Information further identifying the individual is not used. A purchase at a shop, for example, might be made under a one-time-use pseudonym; for a series of transactions comprising an ongoing relationship, such as a bank account, a single pseudonym could be used repeatedly. Although the pseudonyms cannot be linked, organizations will be able to ensure that the pseudonyms are not used improperly by such measures as limiting individuals to one pseudonym per organization and ensuring that individuals are held accountable for abuses created under any of their pseudonyms. Individuals will be able to authenticate ownership of their pseudonyms and use

Resource One (1973)

The “People’s Computing Center”/
Community Memory

First computerised public bulletin
board system (BBS)



Cypherpunks (1980-1990s)

Jude Milhon

"St. Jude"

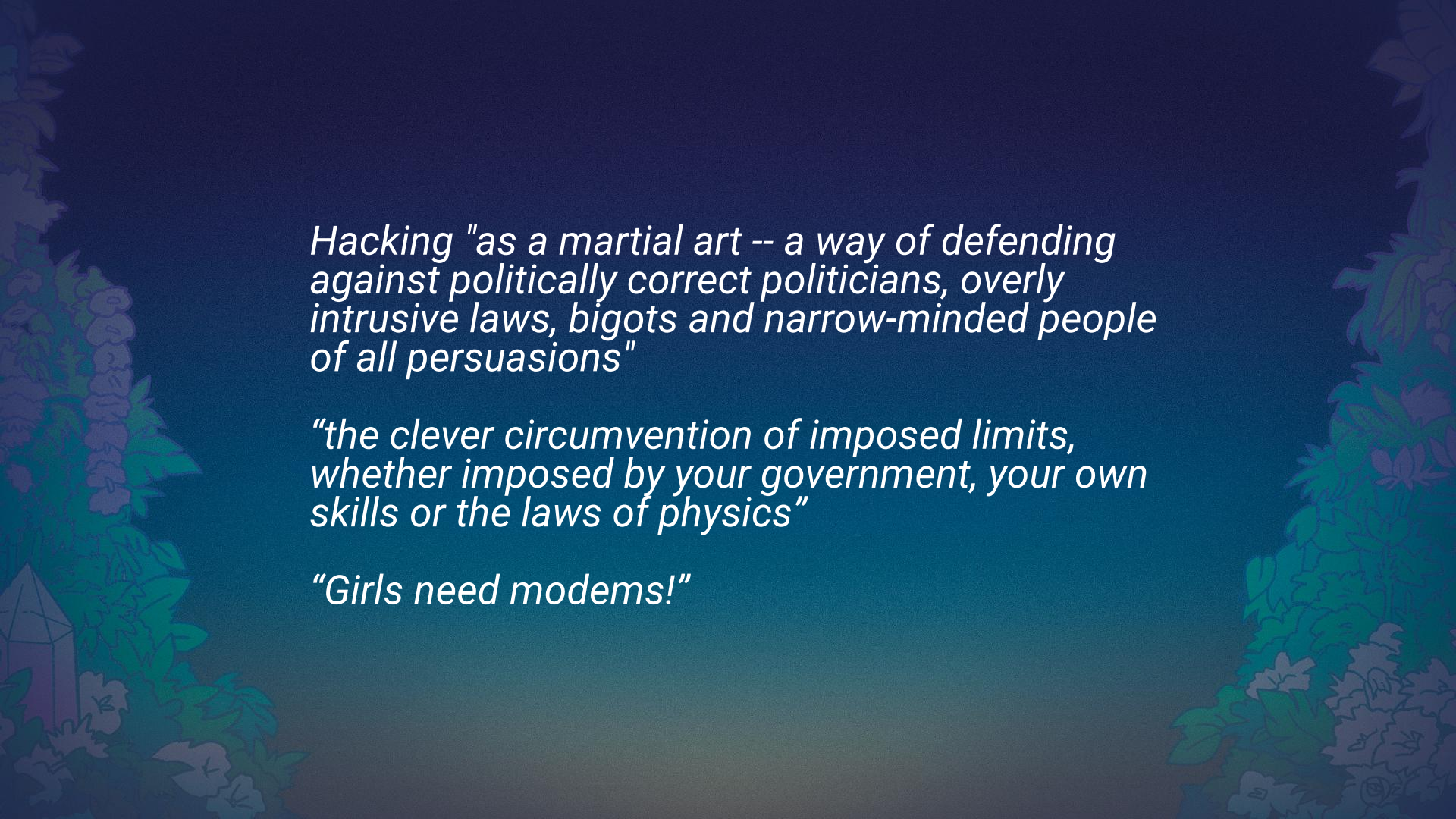
Originator of "cypherpunk"

Founding member of
cypherpunk mailing list

Civil Rights Activist

Senior editor @ Mondo 2000
(now Wired).





*Hacking "as a martial art -- a way of defending
against politically correct politicians, overly
intrusive laws, bigots and narrow-minded people
of all persuasions"*

*"the clever circumvention of imposed limits,
whether imposed by your government, your own
skills or the laws of physics"*

"Girls need modems!"

The Joy of Hacker Sex

*How to Mutate & Take Over the World: an
Exploded Post-Novel (1997) (with R. U.
Sirius)*

*Cyberpunk Handbook: The Real Cyberpunk
Fakebook (1995)*

*Hacking the Wetware: The NerdGirl's Pillow
Book (1994)*

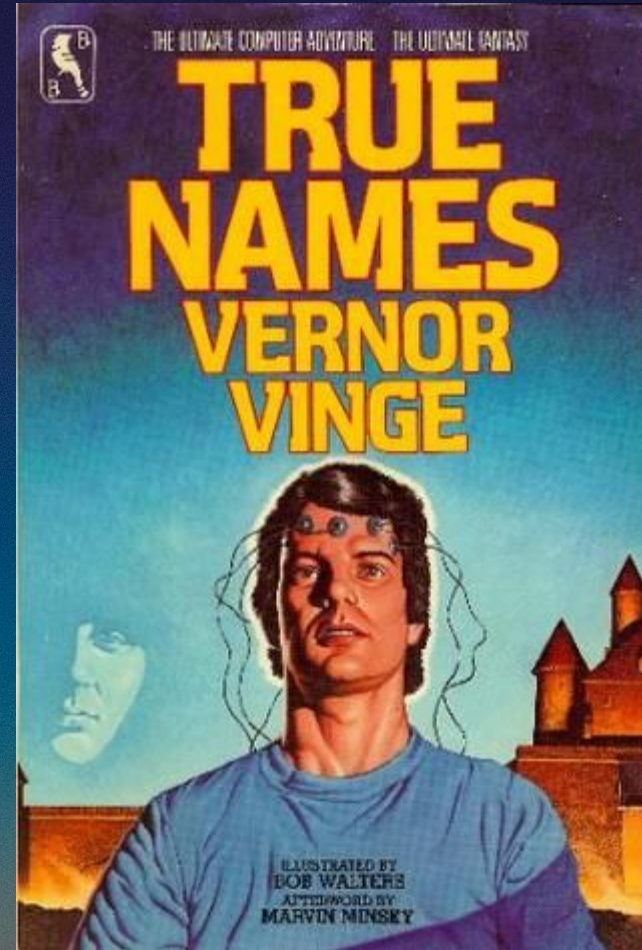
“True Names”

By Vernor Vinge (1981)

Original use of “nym”

Predictive of government
surveillance of parallel online spaces

Mathematics & CompSci Professor



“True Nyms and Crypto-anarchy”

by Tim May (1996)

*“A specter is haunting the modern
world, the specter of crypto anarchy.”*

Founding member of cypherpunks
mailing list, physicist at Intel.

Crypto-anarchist manifesto



"Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner.

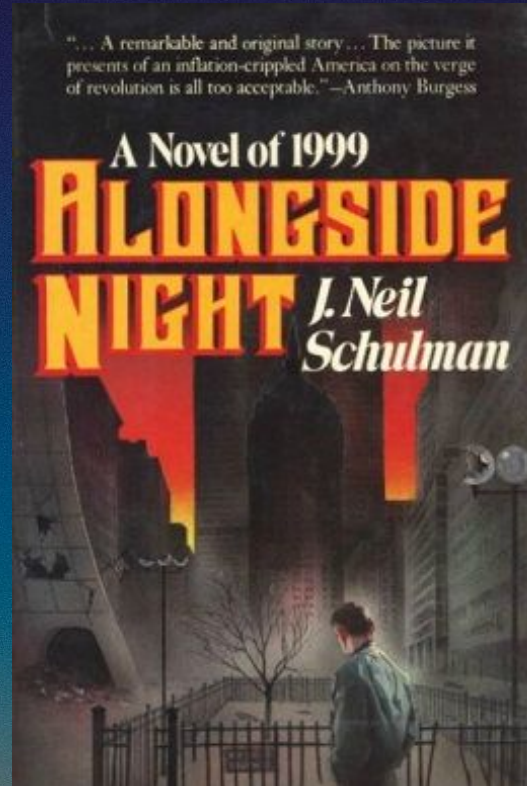
Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering."

Agorism

Counter-Economy:
dual-power black
market-based anti-
statism

<https://agorism.xyz>

Samuel Konkin III
*New Libertarian Manifesto,
An Agorist Primer*



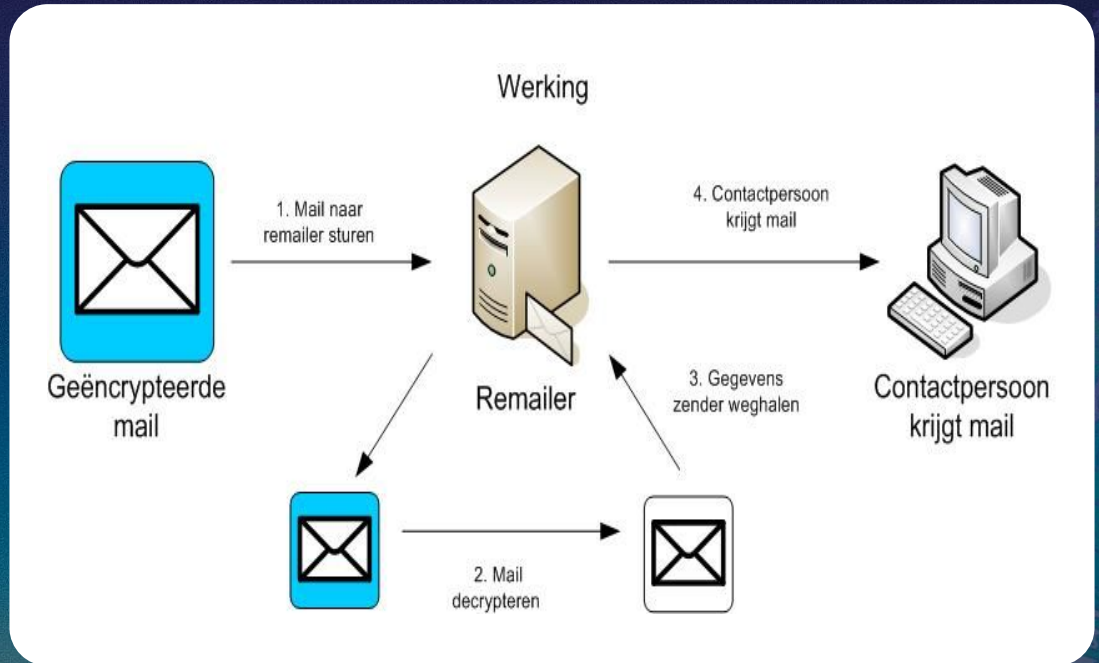
Internet vs. Church of Scientology

(1994 leaks and Penet remailer shutdown)



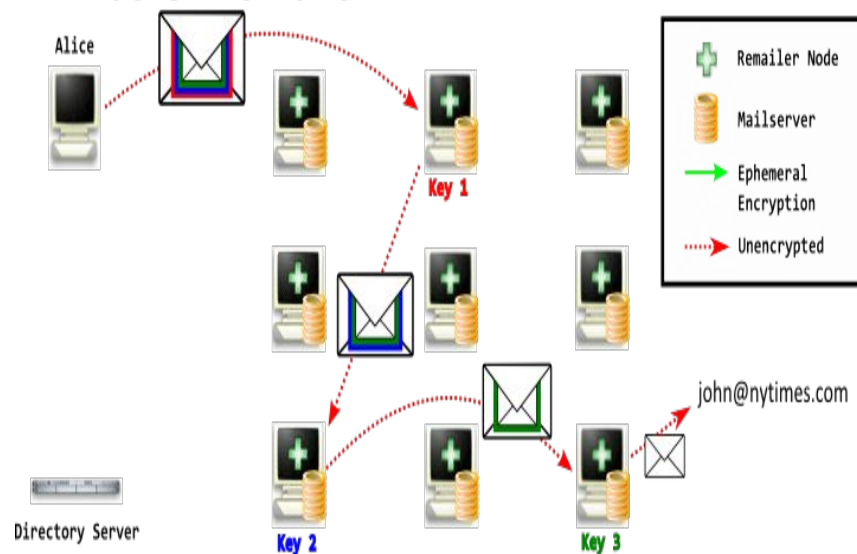
Cypherpunk Anonymous Remailer (1995)

Just PGP!
Led to “proof of work”



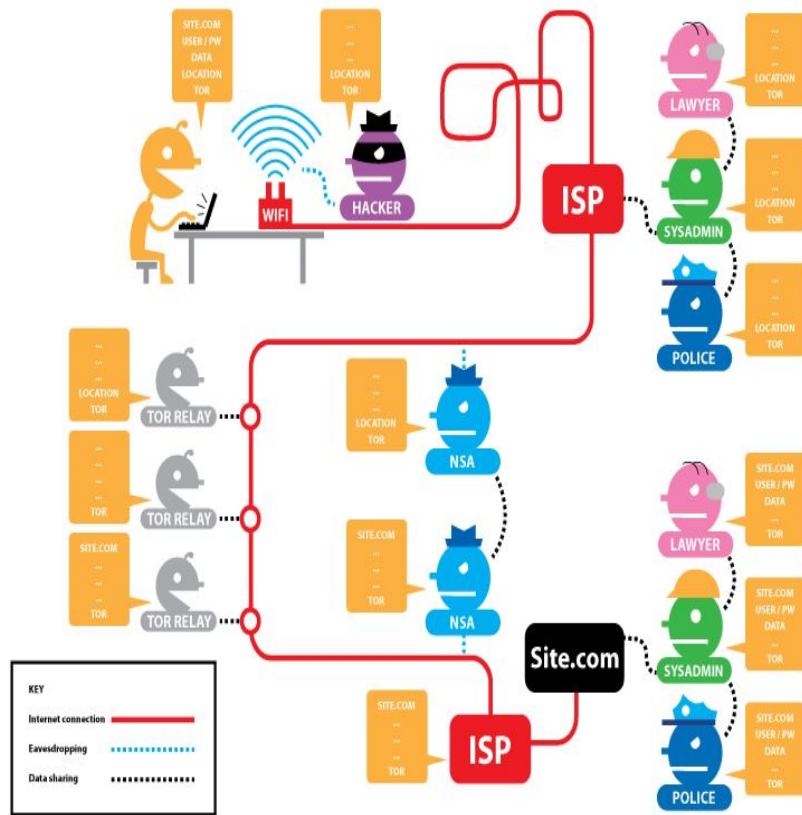
Lance Cottrell
and Len Sassaman

Lance Cottrell
and Len Sassaman



Tor: The Onion Router Systems (2003)

Roger Dingledine, Nick Mathewson, Paul Syverson



Wikileaks (2008)

Assange DAO (2022)

ASSANGE DAO

Our Mission

The mission of the AssangeDAO is to inspire a powerful solidarity network and fight for the freedom of Julian Assange.

We, the cypherpunks, are rallying to the cause of a fellow cypherpunk in distress.

'One of the best ways to achieve justice is to expose injustice.'

— Julian Assange

Anonymous (2011)

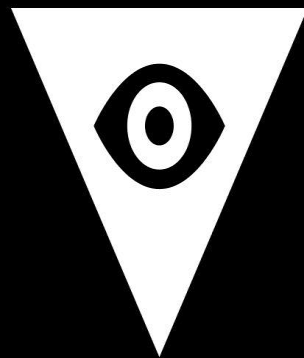


**Faircoin, Unsystem, Dark
Wallet, DarkFi ...**

<https://dark.fi/>

**See: Lunarpunk Engame:
Rachel-Rose O'Leary
Wednesday November
13th 4pm
Devcon Stage 6**

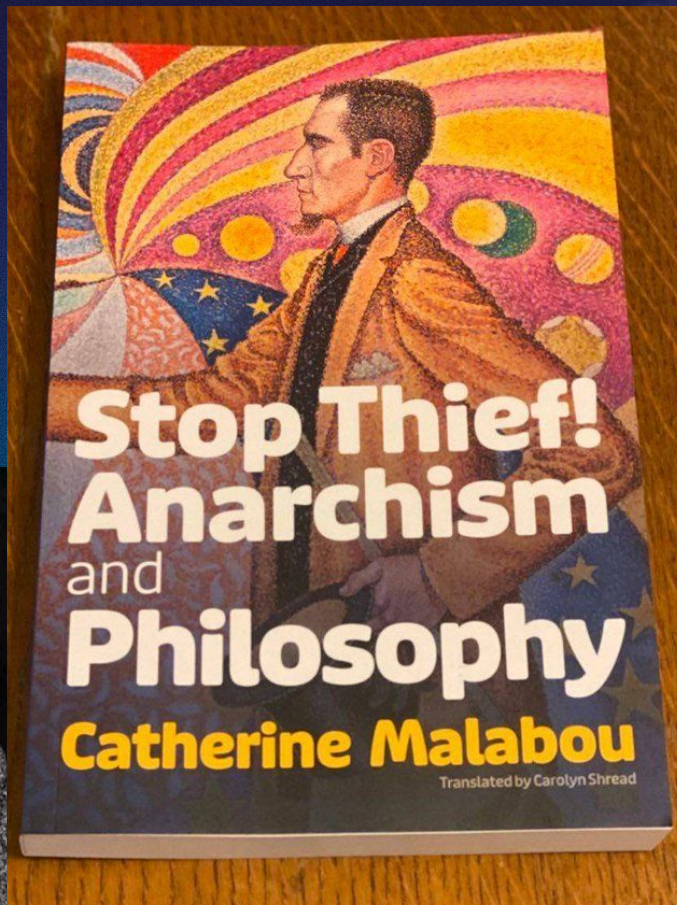
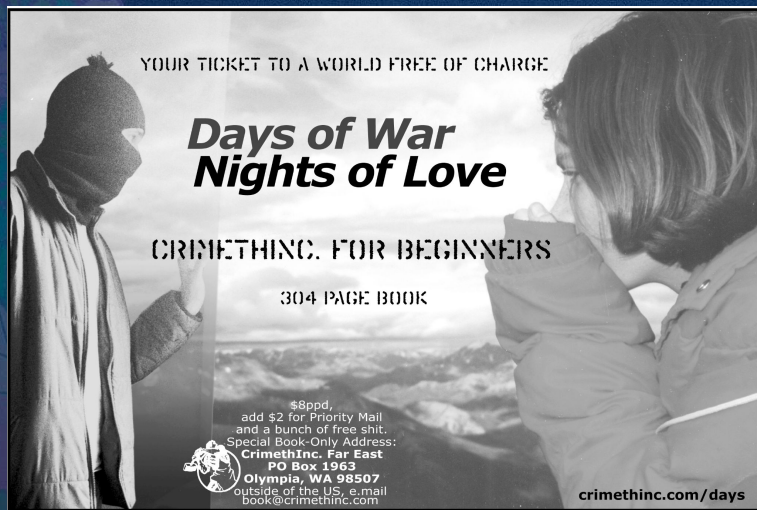
Darkwallet



Anarchism Resurgent

Catherine Malabou

Reiner Schurmann



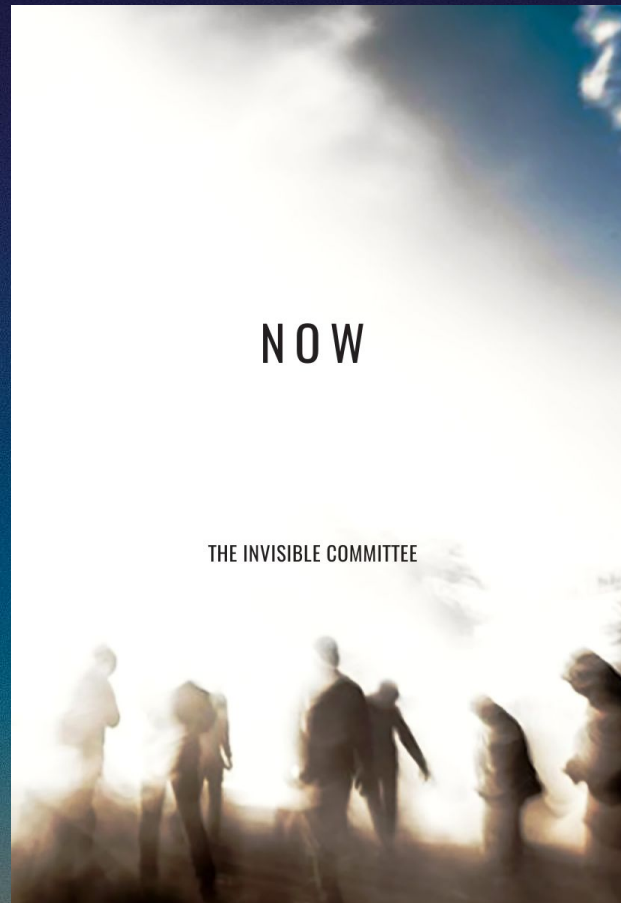
Practical Questions for Revolutionaries

The Cybernetic Hypothesis

Tiqqun

The Cybernetic
Hypothesis

semiotext(e)
intervention
series □ 28



Philosophy of Cypherpunk & Anarchism

Decentralization of Power:

Sovereignty moves from nation-state to the individual/city/province; universal to all humans.

Voluntary Association:

Via contracts and market structures, without domination and exploitation. Freedom of Speech.

Selective Disclosure based on Strong Anonymity:

Information is private by default, agency over sharing.

CYPHERPUNK TECH:

The Holy Grail of Privacy supported by the cypherpunks, but not deployed yet...

MIXNET

A mixnet **prevents traffic analysis** by an adversary capable of watching the entire network, including the NSA. *The Nym mixnet solves this.*



ELECTRONIC CASH (E-CASH)

Digital cash that can't be controlled by a single nation-state. Bitcoin solves this. Designs like Monero/Zcash add **privacy**. *Decentralized fast private e-cash is still needed.*



ANONYMOUS CREDENTIALS

Allow anyone to **selectively disclosure** arbitrary characteristics about themselves like name and wage, similar to e-cash but generalized **zk-nyms** solve this.

Consequences for Ethereum

Identification not Identity:

Just say “no” to Soul-Bound Tokens, DIDs, Self-Sovereign Identity, and other identity systems. Instead, support anonymous credentials/ZKs

Privacy On-Chain - not succinctness bullshit:

“Transparency for the powerful, privacy for the weak”

Via private smart-contracts (Dark.Fi, Aleo ...), Aztec, Tornado Cash - support our prisoners like Roman Storm, Roman Semenov, Alex Pertsev!

Mixnets for Network Privacy/Censorship-Resistance:

Useful to defend validators from each other and clients from RPC, likely needed for inclusion lists - and don't forget Virgil Griffith! See Roger Dingleine's keynote and donate to Tor: <https://torproject.org>

Thank you!

nymtech.net

Harry Halpin

harry@nymtech.net
@harryhalpin

Max Hampshire

max@nymtech.net
@_wjth

