The Cryptoanarchy Technology Pyramid

Frank Braun

@thefrankbraun

2018-10-26

Cryptoanarchy

> *"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. [...] These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."*
> — *Timothy C. May, A Crypto Anarchist Manifesto, 1988*

- Cryptoanarchy is **not** a philosophical utopia, but the attempt to shape life and society with **disruptive technologies**
- Fork in the road: total surveillance state or a cryptoanarchist libertopia?

$\Rightarrow$ People with computers vs. the state

What is Cryptoanarchy? (30 years later)

J. "smuggler" Logan, The Project of Cryptoanarchy, 2018:

"The realization of anarchy by means of cryptography."

- "Cryptoanarchism undermines observation and attribution, and is ultimately subversive."
- "Technologies of non-attribution, untraceability, opaqueness and confidentiality are the political tools of Cryptoanarchy."

Cryptoanarchy mission

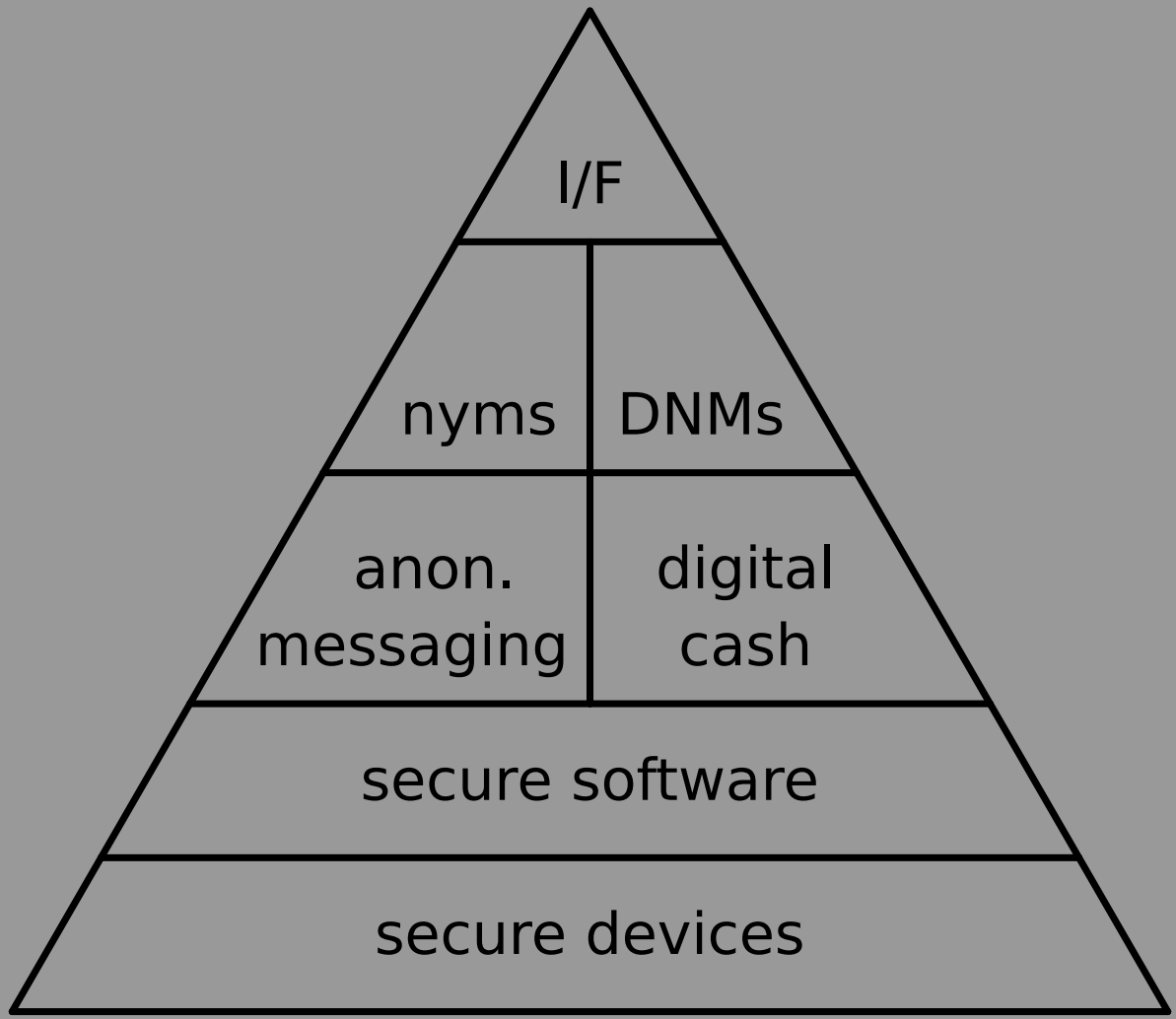
Build an unobservable and non-attributable economy from scratch.

This presentation is neither:

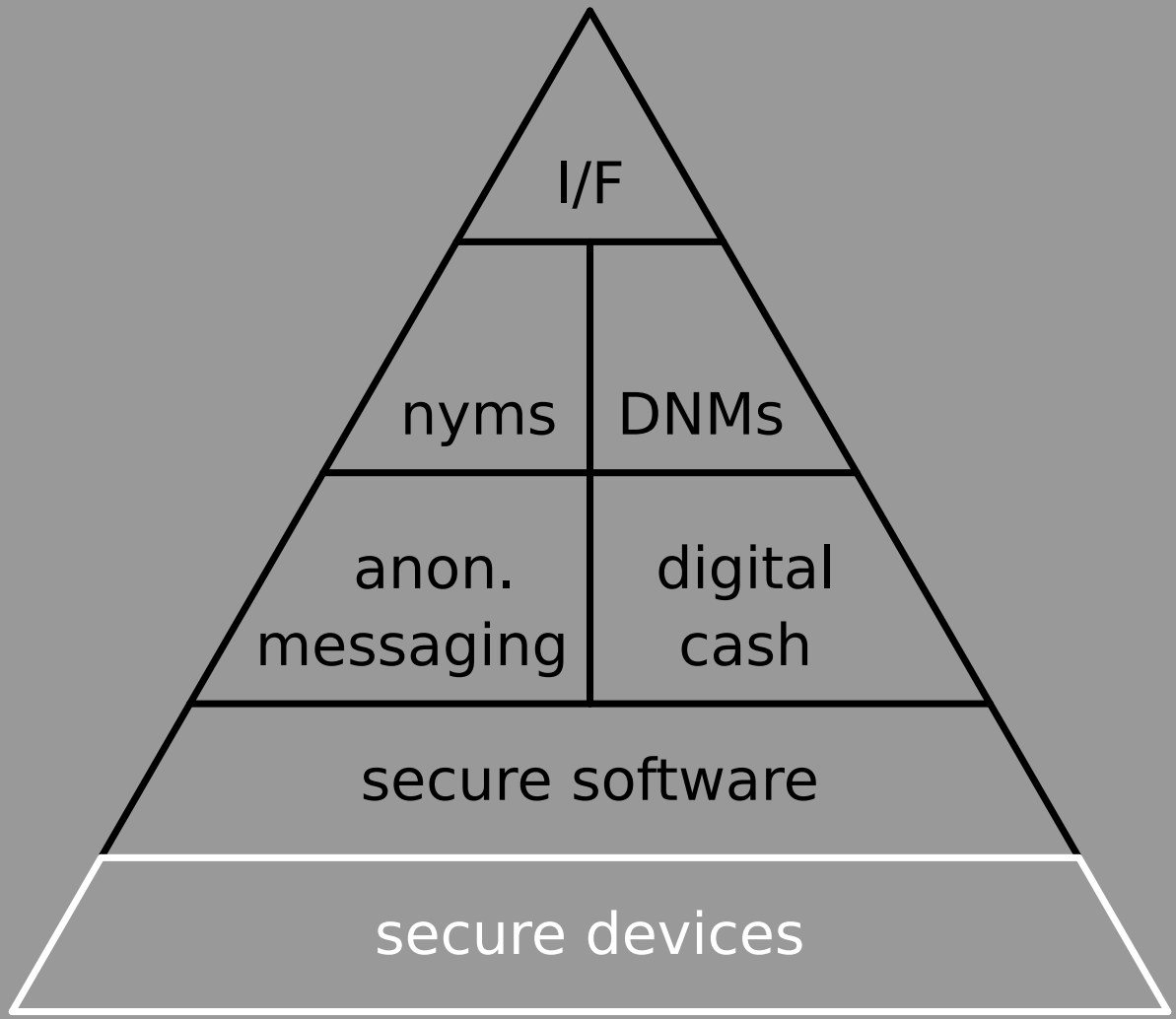
- comprehensive,
- rigorous,
- scientific,
- polite,
- balanced,
- or Bitcoin maximalist,

nor does it try to be.
This rant will cover a very large area, take the best, leave the rest!

The Cryptoanarchy Technology Pyramid / Stack



secure devices



processor level (the good)

processors:

- RISC-V: free and open RISC instruction set architecture
- Intel Software Guard Extensions (SGX): allows user-level code to allocate private regions of memory, called enclaves, that are protected from processes running at higher privilege levels
- AMD Secure Memory Encryption (SME): Uses a single key to encrypt system memory. When enabled in the BIOS, memory encryption is transparent and can be run with any operating system.
- AMD Secure Encrypted Virtualization (SEV): Uses one key per virtual machine to isolate guests and the hypervisor from one another.
- Direct Anonymous Attestation (DAA): a cryptographic primitive which enables remote authentication of a trusted computer whilst preserving privacy of the platform's user.

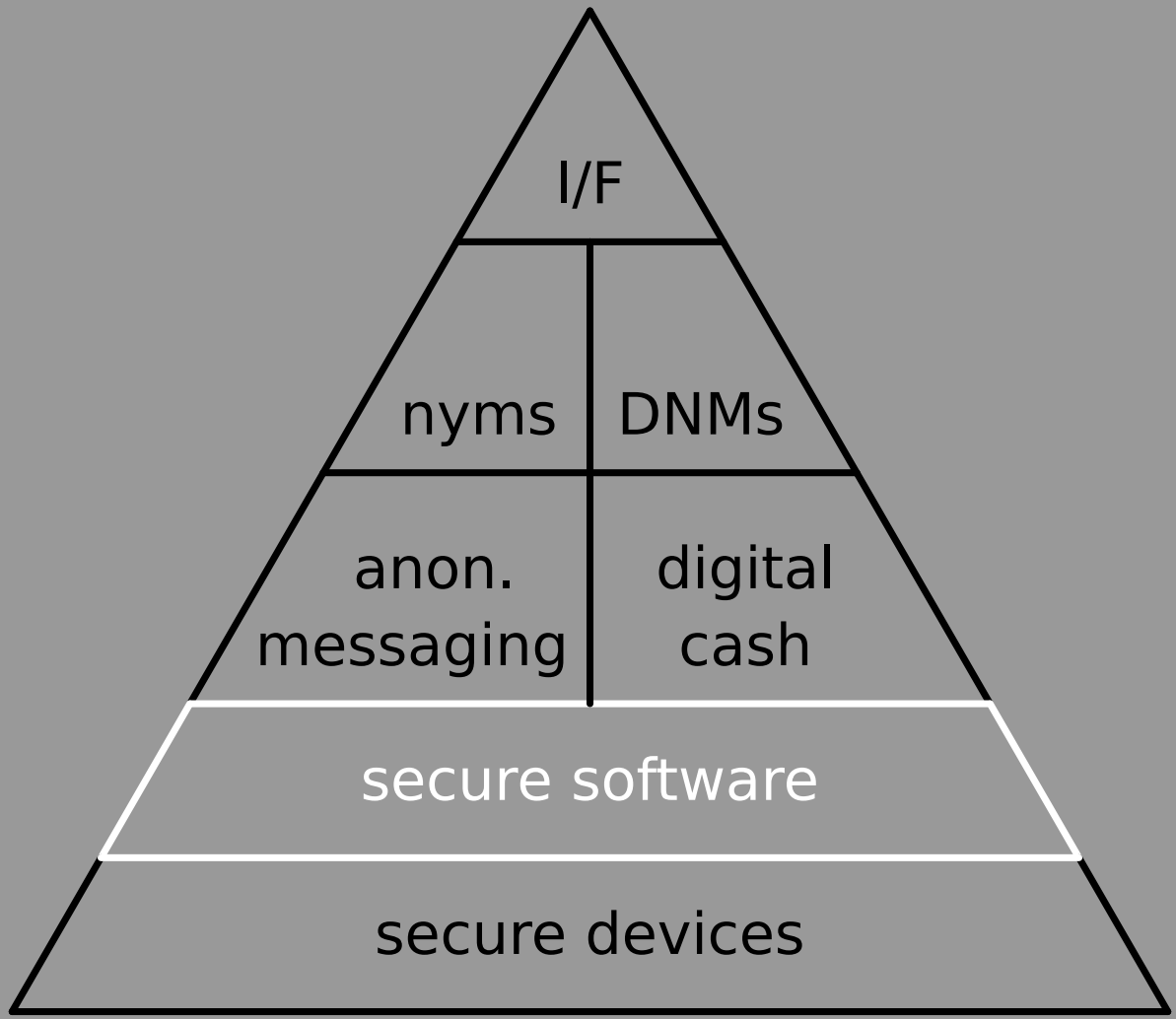
processor level (the bad)

- Intel bugs (Meltdown and Spectre)
- Intel Management Engine (ME)
- baseband processors with proprietary operating systems!

system level (the good)

- open-hardware movement
- Maker culture, Arduino
- Raspberry Pi
- coreboot
- Purism

secure software



operating system level

- OpenBSD: monolithic kernel
- Qubes OS: "microkernel" with Xen hypervisor (problematic)
- MirageOS: library OS to construct unikernels

programming language level

practical:

- Golang
- OCaml

research:

- F*
- CakeML (verified implementation of significant subset of Standard ML)
- Ivory/Tower
- Idris

specifications / model checking:

- TLA+

formal verification (examples)

- F* used to create HaCl*, a formally verified cryptographic library, and miTLS, a formally verified reference implementation of TLS, as part of Project Everest.
- Ivory/Tower used in DARPA's HACMS program to create unhackable hardware (drones):

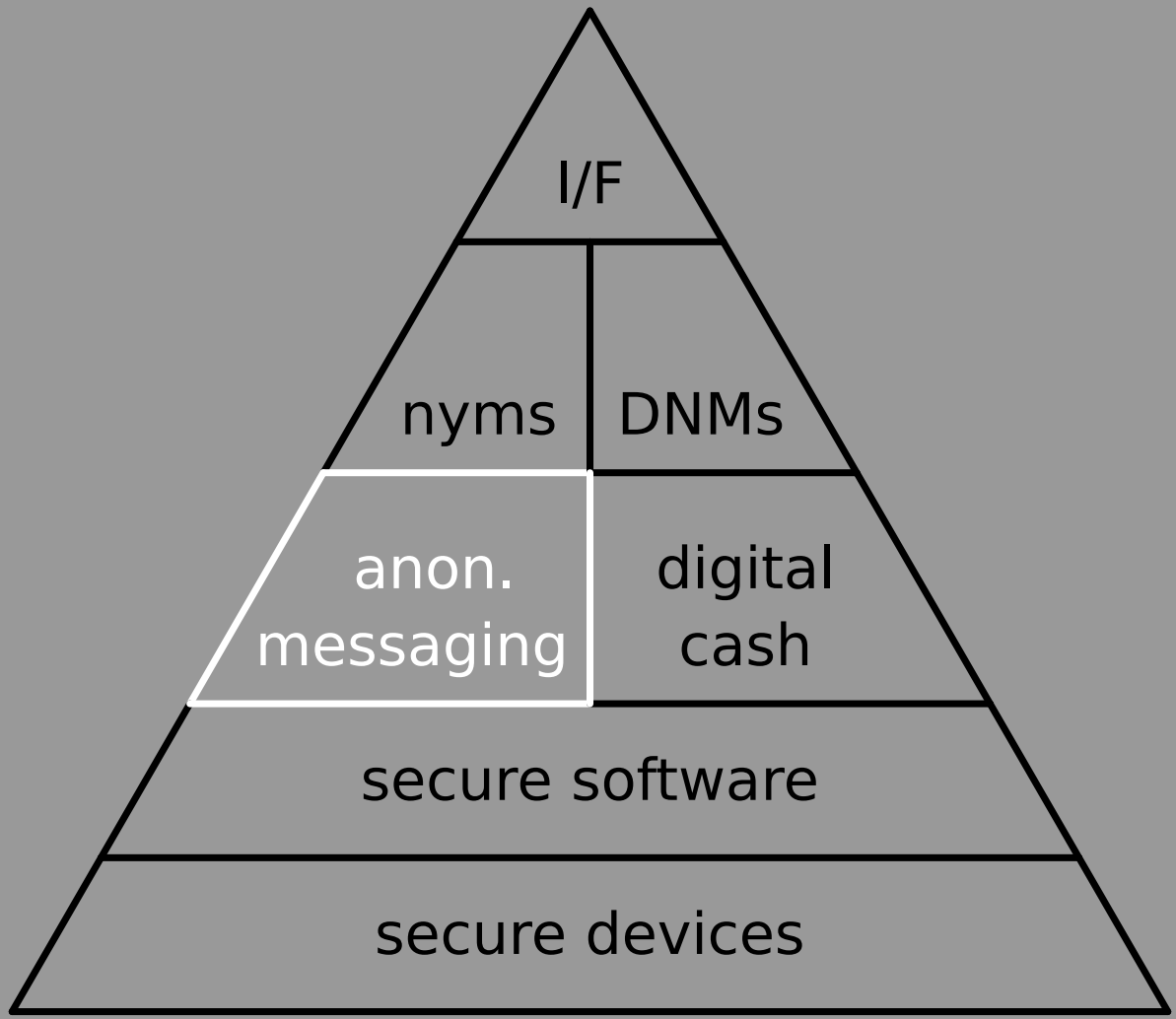
  "The HACMS Red Team was given six weeks and full access to the source code for both vehicles to evaluate their cyber security claims. They were unable to compromise the security of either vehicle."
  —http://loonwerks.com/projects/hacms.html

tooling level

- Git distributed version control
- collaboration tools
- secure code delivery with multi-party signatures

→ Codechain

anonymous messaging



anonymous messaging (theory)

Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two
D. Das, S. Meiser, E. Mohammadi, and A. Kate,
Cryptology, Report 2017/954

Abstract: This work investigates the fundamental constraints of anonymous communication (AC) protocols. We analyze the relationship between bandwidth overhead, latency overhead, and sender anonymity or recipient anonymity against **a global passive (network-level) adversary**. We confirm the trilemma that an AC protocol can only achieve two out of the following three properties: strong anonymity (i.e., anonymity up to a negligible chance), low bandwidth overhead, and low latency overhead.

anonymous messaging (mix networks)

- around forever: David Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Comm. ACM, 24, 2 (**Feb. 1981**); 84-90
- evolution of remailers:
  - type I: cypherpunk remailers
  - type II: mixmaster remailers
  - type III: mixminion remailers
- **but**: mostly forgotten

anonymous messaging (the good)

This slide unfortunately left blank.

anonymous messaging (the bad)

- XMPP+OMEMO over Tor (best of the bad)
- Signal (why do you want my phone number, Moxie?)
- WhatsApp (the messenger abandoned by its founder, really?)
- Telegram (roll your own crypto, seriously?)
- Facebook Messenger (I shoot myself now)
- ...

(not considered here: Matrix, Riot, Keybase, Threema, etc.)

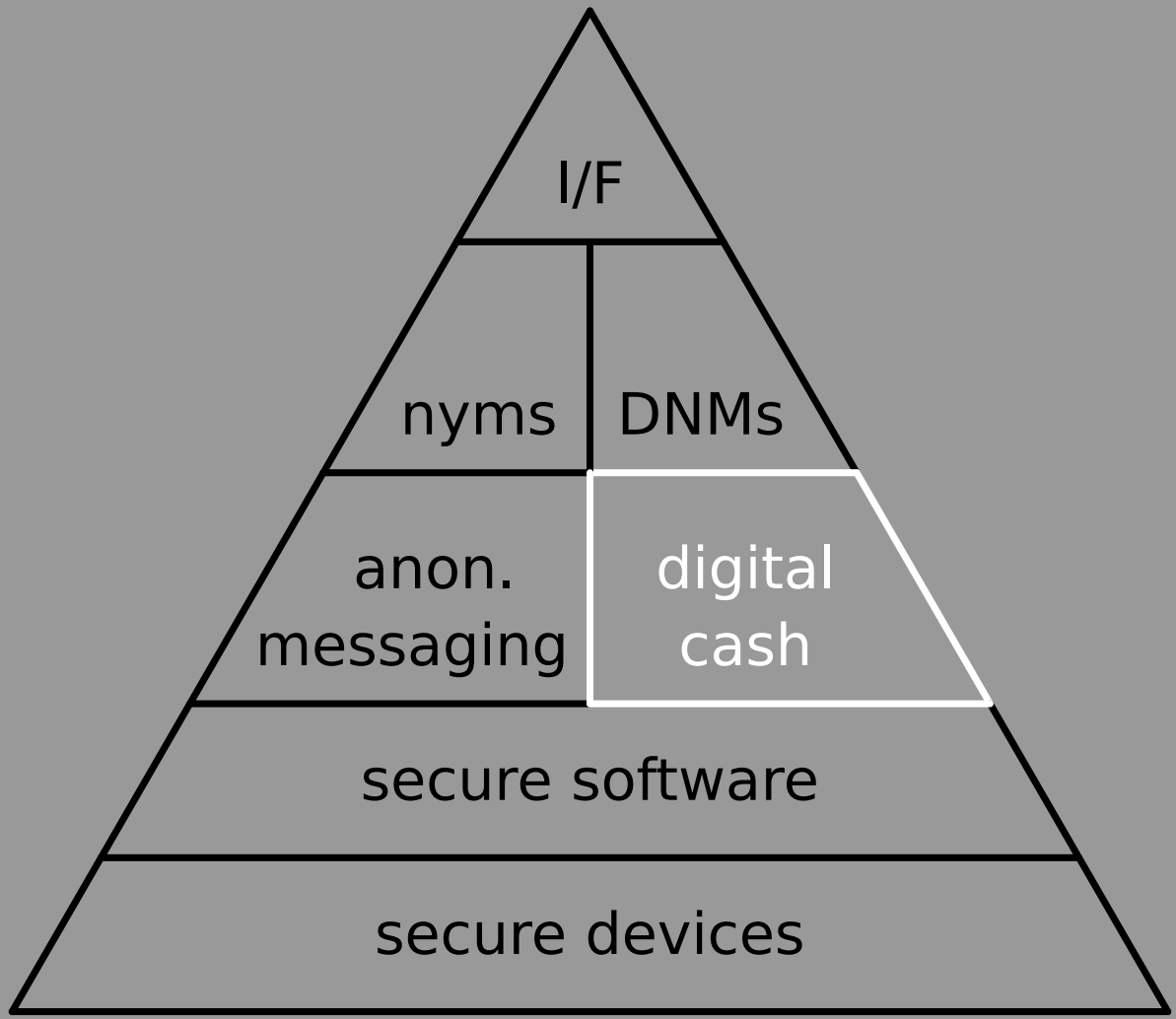
anonymous messaging (the ugly)

Tor:

- Greatest detriment to anonymous messaging ever invented.
- You couldn't build a better honey trap, if you wanted to.

'Nuff said.

digital cash



what is money?

definition:

- medium of exchange (3 Euro exchanged for Döner)
- unit of account (your total balance is 2.56 Euro)
- store of value (Krugerrand under mattress)

features:

- portability (cattle are not portable)
- divisibility (cattle are not divisible)
- durability (tea is not durable)
- rarity (sand is not rare)
- fungibility (diamonds are not fungible)

what is digital cash?

anonymous electronic money

DigiCash (1990 – 1998)

cryptographer David Chaum:

- Untraceable electronic mail, return addresses, and digital pseudonyms, Comm. ACM, 24, 2 (**Feb. 1981**); 84-90

⇒ groundwork for anonymous communications research

- **1983**: Blind signatures for untraceable payments, Advances in Cryptology: Proceedings of CRYPTO 82, pp 199-203

⇒ the foundation of **anonymous** digital money

founded DigiCash Inc. in 1990:

- produced "anonymous" micropayment system ecash

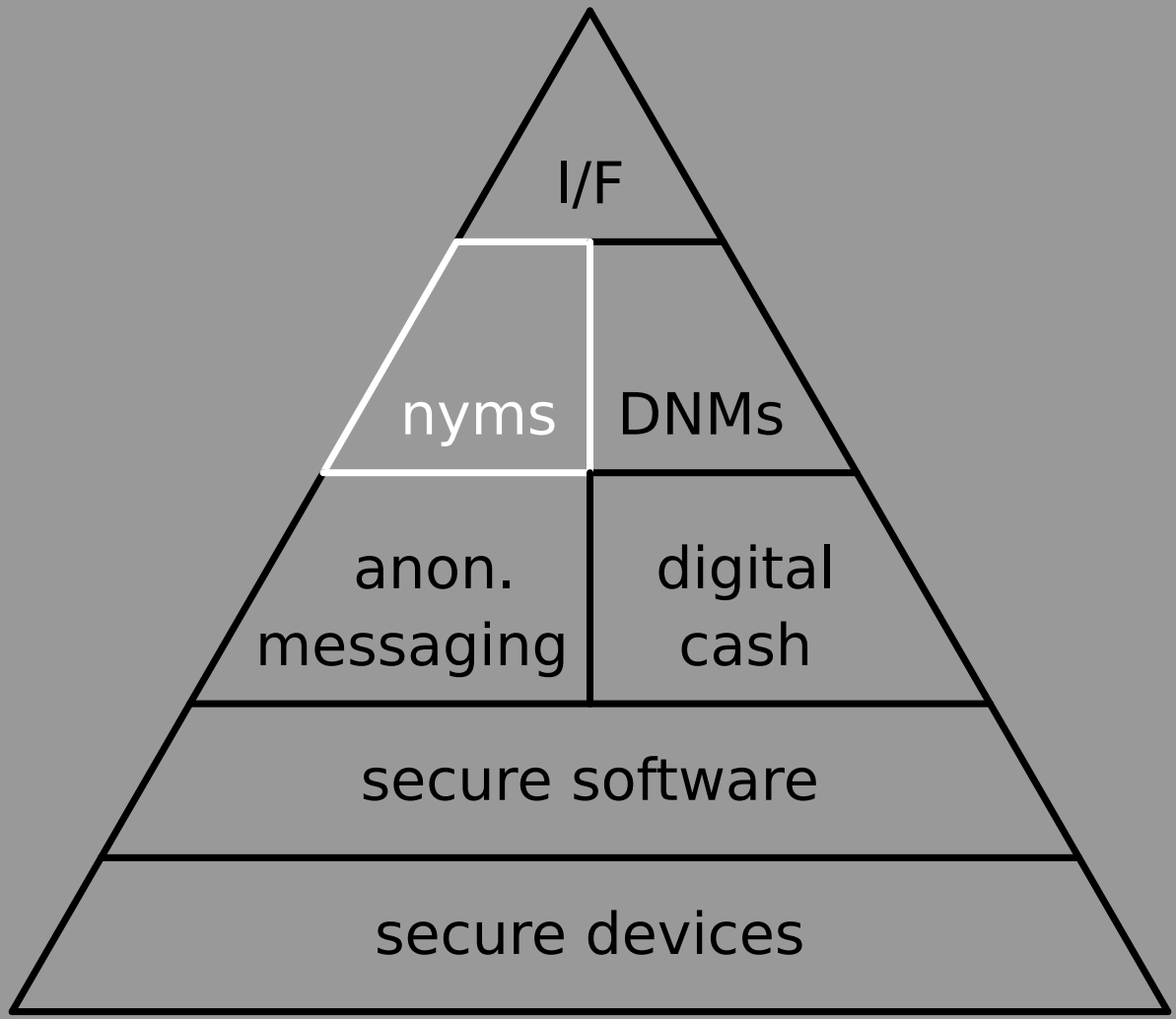
⇒ declared **bankruptcy** in 1998

digital cash (the ugly)

- Bitcoin
- most altcoins[1]
- blockchain in general

[1] Monero & Zcash are half decent

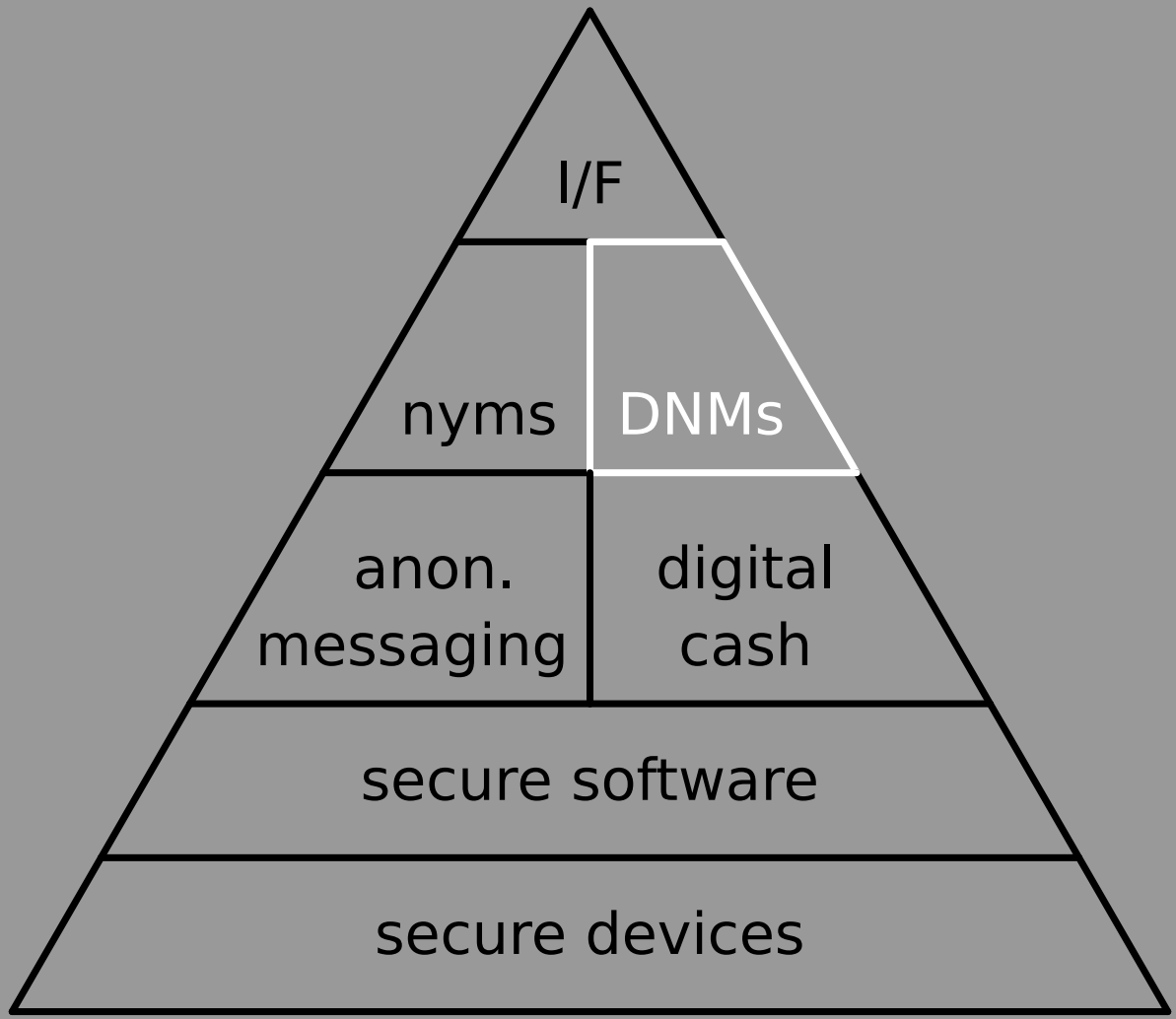
pseudonyms & reputation



pseudonyms & reputation

- provable pseudonyms are necessary to build reputation systems
- expensive pseudonyms would help against exit scams
- PGP is waaaaaaay beyond its shelf life, time to retire it.

dark net markets (DNMs)



dark net markets: state of the art

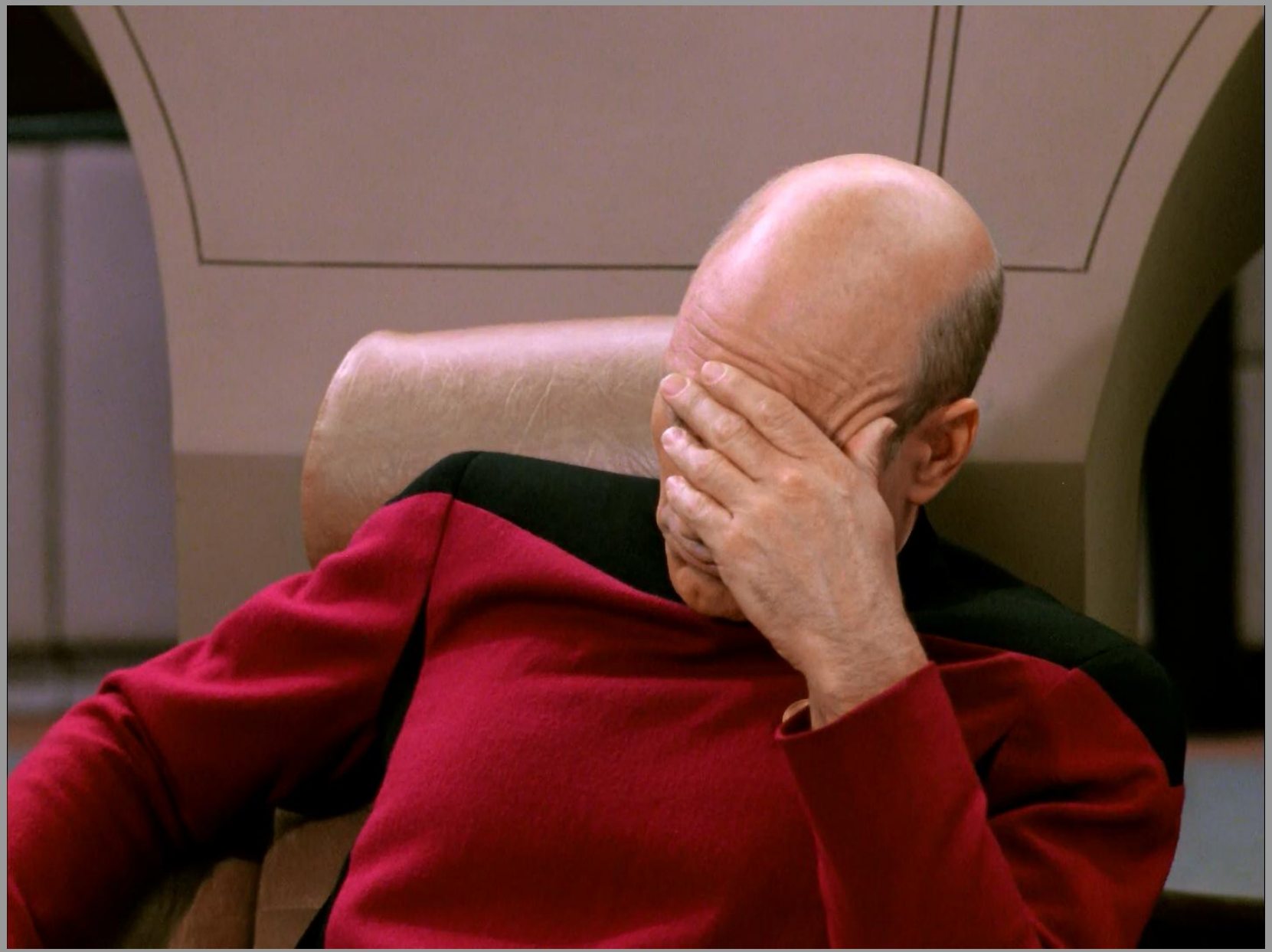
Now we have all our necessary components together.
We take:

- shitty low-latency anonymization technology (Tor)
- encryption and reputation building tech past its due date (PGP),
- a fully traceable and non-fungible digital currency (Bitcoin),

and use it to build a marketplace on a delivery mechanism with:

- huge attack surface,
- that makes it easy to fingerprint users

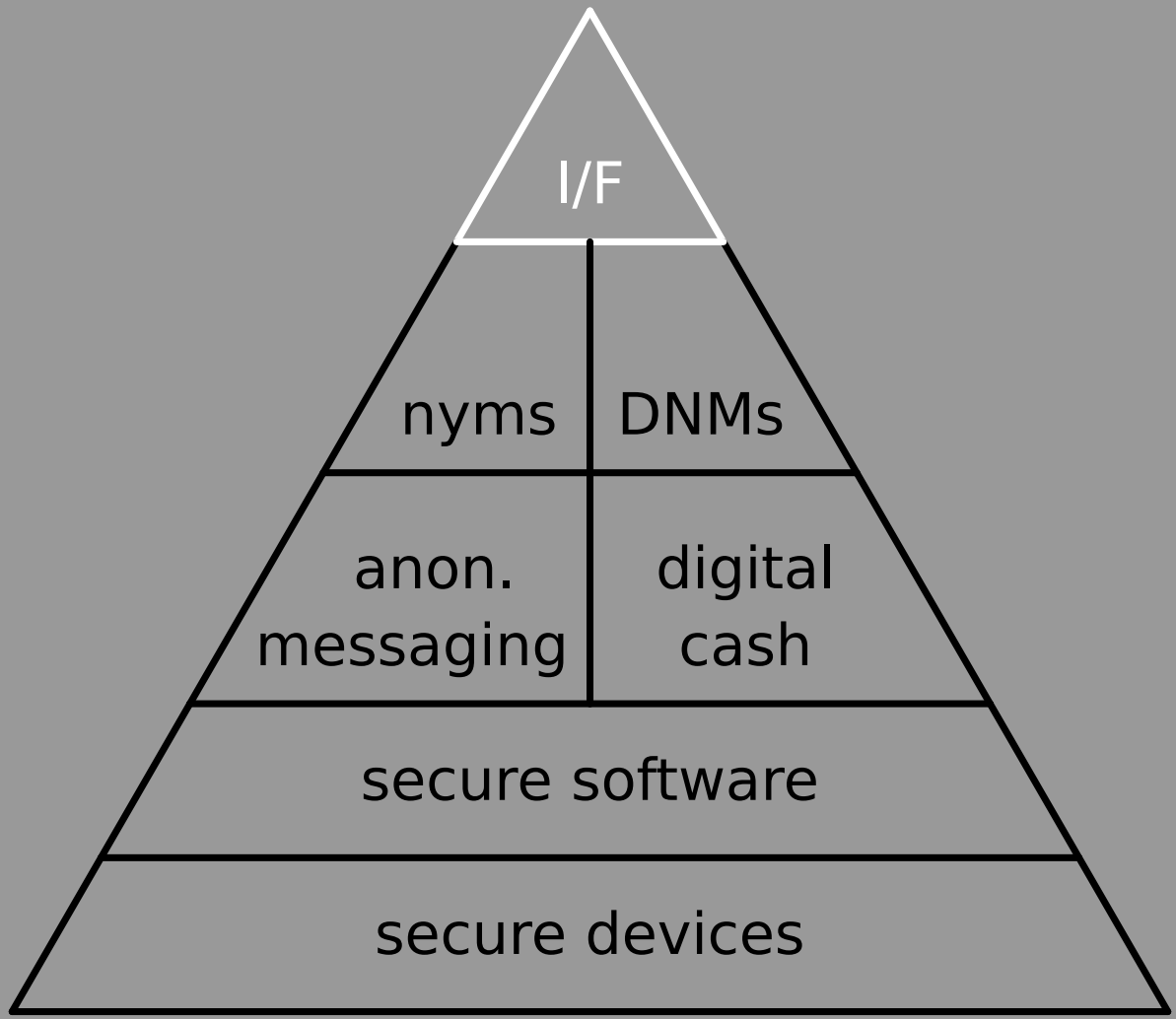
(Tor Browser).



lesson in here

you cannot build a pyramid on quicksand

physical interfaces (I/F)



physical interfaces (I/F)

Shocking news: physical beings operate in the physical world.[2]

[2] And meatspace is a bitch.

physical interfaces (examples)

drones:

- open-source fixed-wing long-distance drones

$\Rightarrow$ total disruption of smuggling (a.k.a. as "your ticket to fame")

- physical mix nets for drones
- drone drop shipping

physical structures:

- trading rooms
- Faraday bar
- T.A.Z.: The Temporary Autonomous Zone, Hakim Bey, **1991**

$\rightarrow$ Smuggler's talk tomorrow

dissecting the pyramid

1. things are moving on the secure devices and secure software layer (but that's common CS research, often military funded)

2. not much has been achieved on the core Cryptoanarchy layers in the last 30 years:
   - we got stuck with PGP
   - applied anonymization shifted to low-latency networks (Tor)
   - current blockchain hype is derailing anonymous digital cash

3. meatspace has been ignored for way to long in Cryptoanarchy theory[3] and practice

[3] counter-example: The Second Realm - Book on Strategy, Smuggler, **2010**

conclusion

1. half-assing is not going to cut it
2. we need a paradigm shift to high-latency systems
3. don't ignore the wetware

ask yourself:

Do I want to live in a comic book dystopia or do I want to be a free human being?

final thoughts

Timothy C. May, 2018:

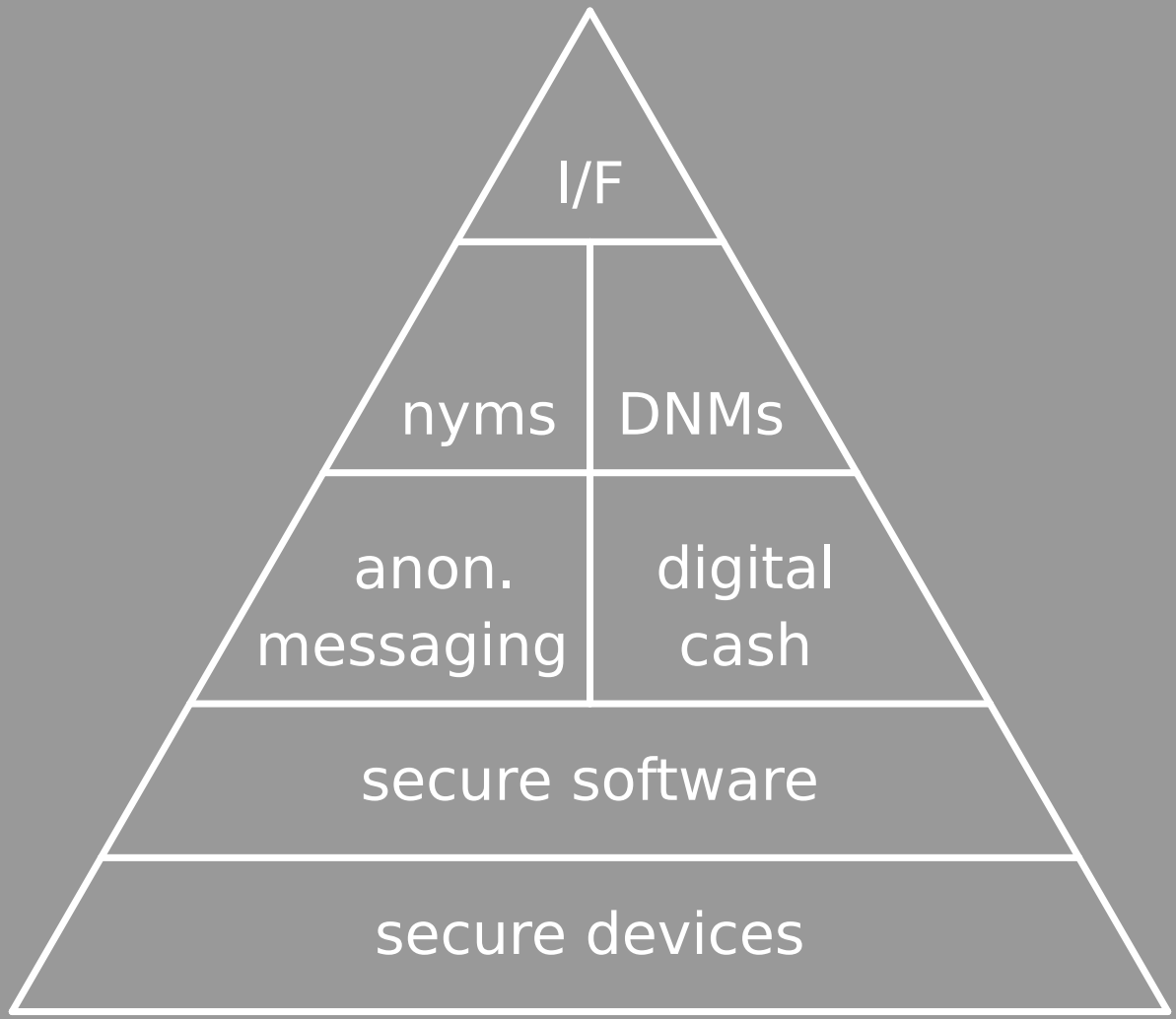
- "Don't use something just because it sounds cool...only use it if actually solves some problem (To date, cryptocurrency solves problems for few people, at least in the First World)."
- "Most things we think of as problems are not solvable with crypto or any other such technology (crap like 'better donation systems' are not something most people are interested in)."
- "If one is involved in dangerous transactions – drugs, birth control information – practice intensive 'operational security'...look at how Ross Ulbricht was caught."

final thoughts (cont.)

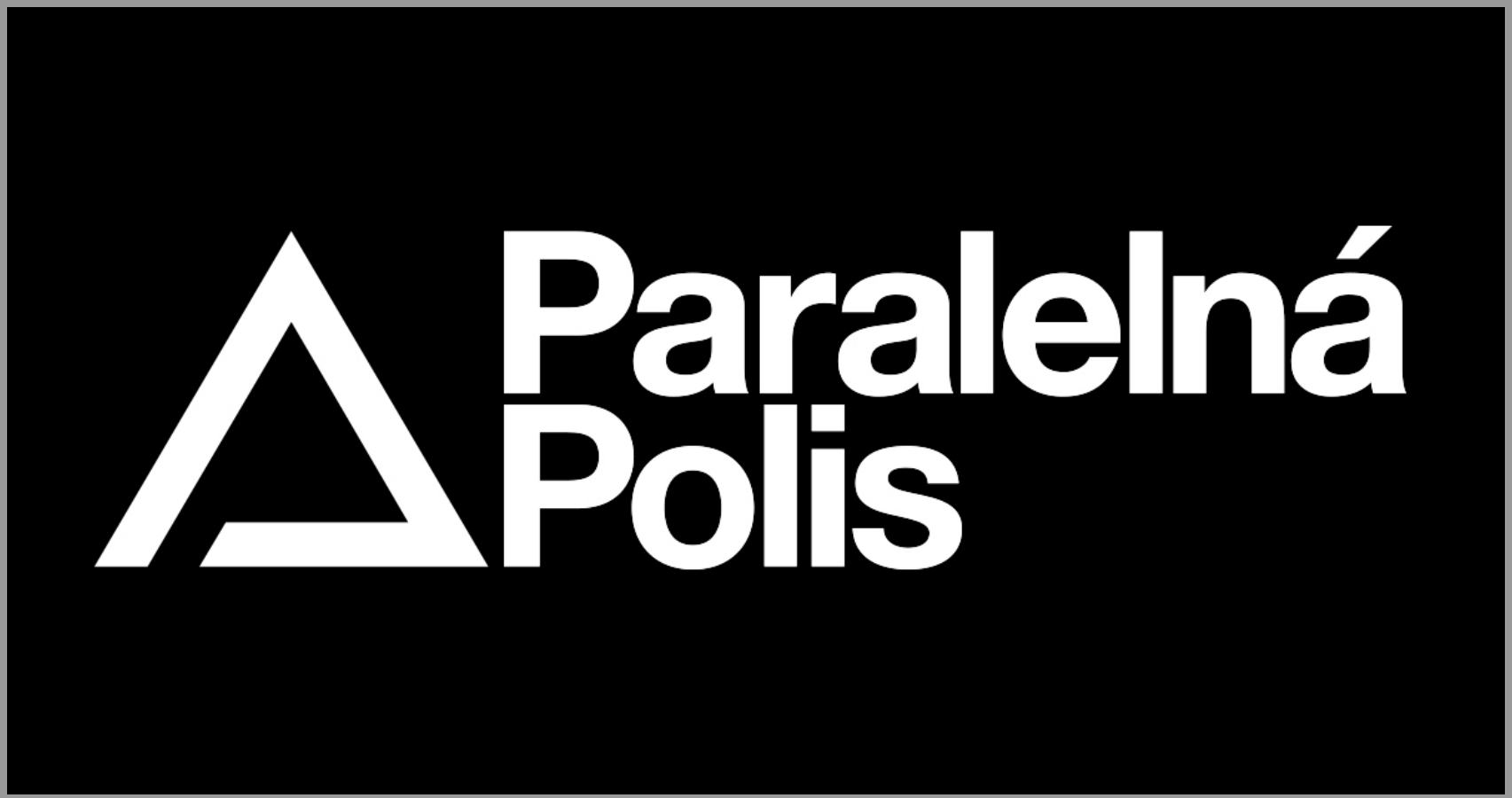
Timothy C. May, 2018:

- "Mathematics is not the law"
- Crypto remains very far from being usable by average people (even technical people)
- Be interested in liberty and the freedom to transact and speak to get back to the original motivations. Don't spend time trying to make government-friendly financial alternatives.
- Remember, there are a lot tyrants out there.

the future?


I/F
nyms
DNMs
anon. messaging
digital cash
secure software
secure devices

help make it happen!



acknowledgments: J. "smuggler" Logan & Arto Bendiken

contacts:

- Email: `frank@cryptogroup.net` (use PGP, key on keyserver)
- `94CC ADA6 E814 FFD5 89D0 48D7 35AF 2AC2 CEC0 0E94`
- Twitter: @thefrankbraun
- Gab: @frankbraun

slides: `http://frankbraun.org/the-cryptoanarchy-technology-pyramid.pdf`

thank you very much for your attention! questions?