Version 3.0, 2024-06-09 12:45

NURTURING DECENTRALIZATION IN THE AGE OF DIGITAL COMMONS

Matthias Tarasiewicz @parasew
RIAT INSTITUTE

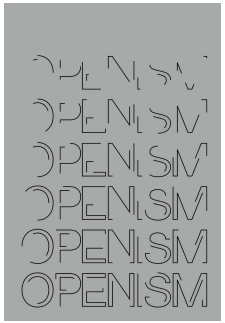
MONERO KONFERENCO, PRAHA 2024

DL SLIDES AT
https://riat.at/monerokon

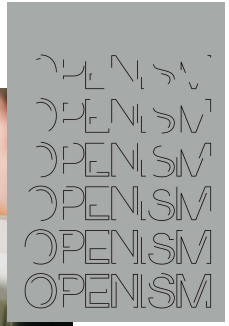

MONERO
KONFERENCO 4
PRAHA - 2024

HELLO WORLD

- Working with free and open source since 1998
- RIAT Institute: an NGO actively participating and documenting open theory and practice since 2004
  - Support R+D in free and open source
  - Foster technological literacy



https://riat.at/publication_pack



The past, present and future of Opt-Out with Open and Libre Hardware #hcpp19, 6th Annual Hackers Congress Paralelni Polis, Prague, October 4, 2019.

Future of Open Hardware in a (Verifiable) Decentralised World (video) Devcon 5, Ethereum Developer Conference, Japan, October 2019.

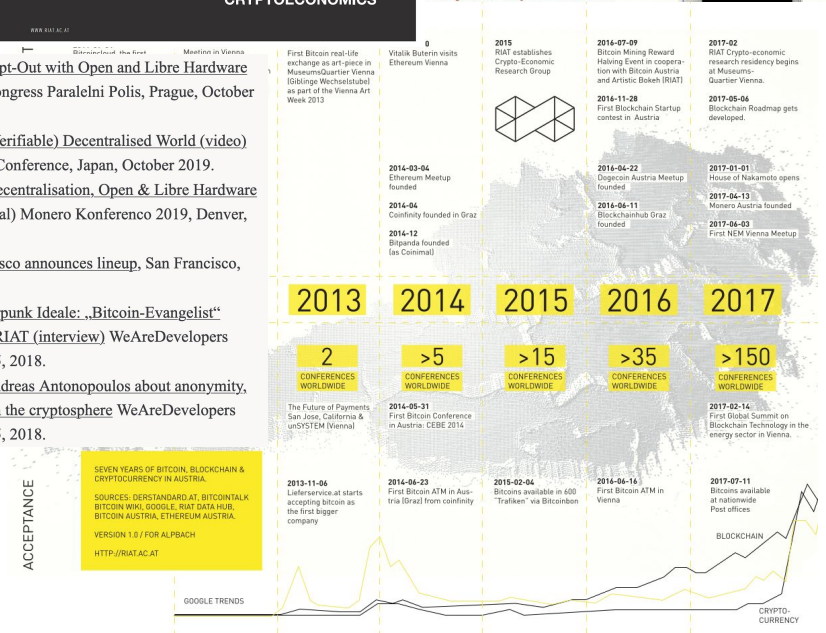
Matthias Tarasiewicz: Critical Decentralisation, Open & Libre Hardware for and with Monero (First Annual) Monero Konferenco 2019, Denver, Colorado, June 22-23, 2019.

Grey Area Festival in San Francisco announces lineup, San Francisco, June 26, 2018.

Anonymität, Privacy und Cypherpunk Ideale: „Bitcoin-Evangelist" Antonopoulos im Gespräch mit RIAT (interview) WeAreDevelopers World Congress, Vienna, June 25, 2018.

Hodling, Buidling, Spedning: Andreas Antonopoulos about anonymity, privacy and sentiment changes in the cryptosphere WeAreDevelopers World Congress, Vienna, June 25, 2018.

v1docq47/**monero-cdc-36c3-transcriptions**



DECENTRAL COMMUNITY

critical decentralisation

→ Critical decentralisation cluster at the annual C3 (Chaos Communication Congress)

→ Transcriptions from 36c3 at https://github.com/v1docq47/monero-cdc-36c3-transcriptions/

→ Videos Critical Decentralisation Cluster (36c3) https://czechmonero.cz/critical-decentralisation-cluster-36c3/

→ Cluster web is here **https://decentral.community**

v1docq47/**monero-cdc-36c3-transcriptions**

STRUCTURE OF THE TALK

DECAY

DECAY, EXIT, VOICE
ENSHITTIFICATION, OLIGARCHY AND ISOMORPHISM

OPEN SOURCE

SOFTWARE IS EATING THE WORLD?
PERMISSIVE LICENSES ARE EATING THE COMMONS

VERIFY ALL THINGS

MODERN TECHNOLOGY IS NOT VERIFIABLE
WHY WE NEED VERIFIABLE THINGS

NURTURE DECENTRALIZATION

CONCLUSIONS

1

DECAY

“Enshittification” (Cory Doctorow)

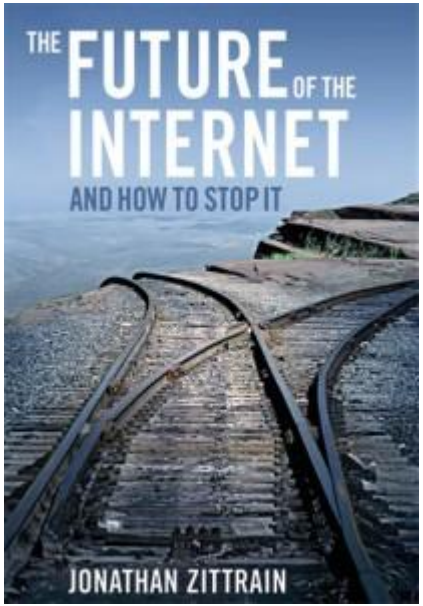
“Enshittification is coming for absolutely everything” (Cory Doctorow)

Enshittification

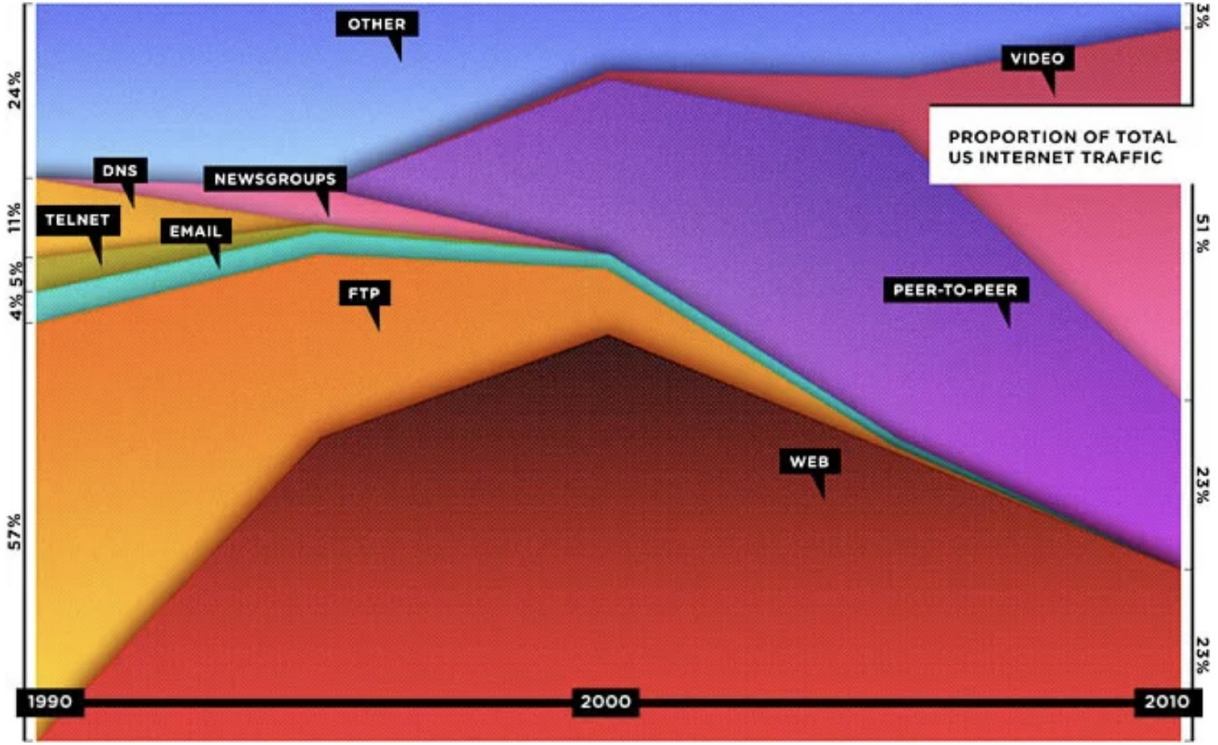
- Online platforms transition through stages where their value proposition shifts focus among users, business customers, and the platform itself, ultimately degrading the user experience.
- Enshittification stages:
  - 1: User-Centric Growth
  - 2: Business-Centric Monetization
  - 3: Self-Centric Extraction
  - 4: Death of the platform

'Enshittification' is coming for absolutely everything. Cory Doctorow, Financial Times, 2024.

“The Future of the Internet and How to Stop it” (Zittrain, 2008)



“The Web Is Dead. Long Live the Internet” (Anderson and Wolf, 2010)



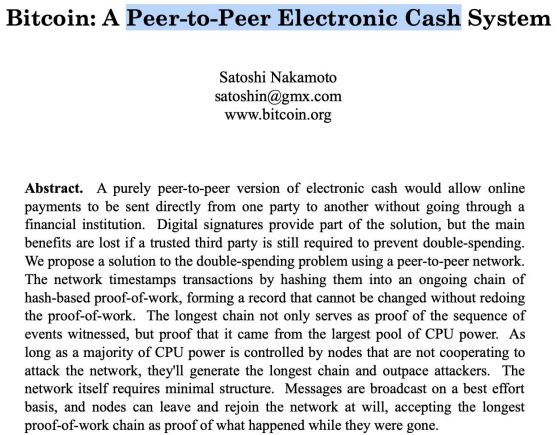
Sources: Cisco estimates based on CAIDA publications ILLUSTRATION: ANDREW ODLYZKO

The enshittification of enshittification

Enshittification, Disenshittification, and the Bezzle: Cory Doctorow in Conversation with Randall Munroe (XKCD)
Maybe enshittification is a good thing. Here's why
Pee Review: The Enshittification of Science?

Enshittification of Bitcoin?

- Until 2008: Online payments have been broken or infested by middlemen (see Paypal)
- 2009: Bitcoin: “online payments to be sent directly from one party to another without going through a financial institution” → **Micropayments**
- 2024: Bitcoin is not used for micropayments, and other cryptocurrencies do not solve this (except Monero).



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

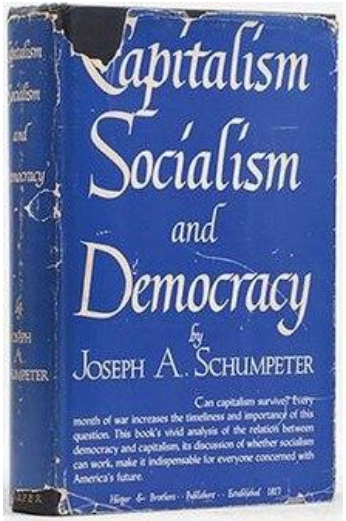
“Today, Bitcoin appears as cryptoanarchistic as a car and provides all the tools to f* you”

(Smuggler at HCPP, 2018).

Schumpeter's Theory of Creative Destruction

- Understanding innovation and its lifecycle
- New innovations disrupt existing industries and economic structures, leading to the creation of new paradigms. As these innovations mature, they often undergo transformations that can shift their original values and goals.

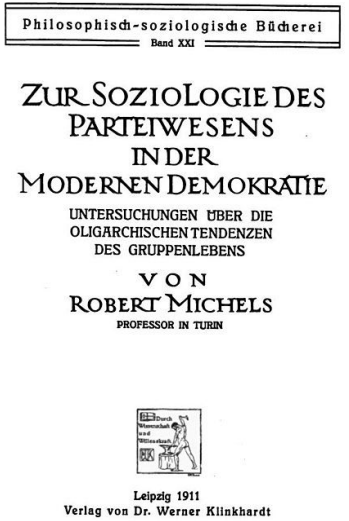
Bitcoin’s initial disruptive vision of a decentralized, digital cash system has evolved into a more mainstream financial asset, influenced by market forces and regulatory pressure.



Joseph Schumpeter
Capitalism, Socialism, and Democracy (1942)

The Iron Law of Oligarchy

- The "Iron Law of Oligarchy," formulated by sociologist Robert Michels in *Political Parties* (1911), suggests that all complex organizations, regardless of how democratic they are at the start, eventually develop oligarchic structures.



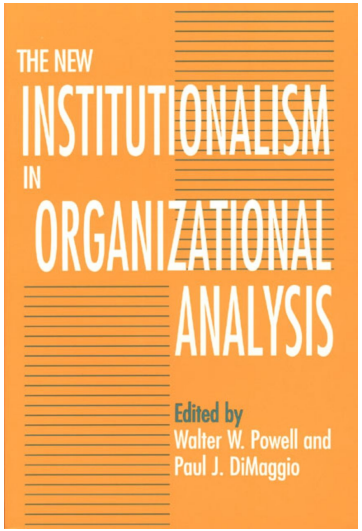
Robert Michelis
Political Parties (1911)

This theory can be applied to understand how the decentralized ideals could decay over time as power becomes concentrated among a few key players, such as major miners, exchanges, and institutions.

Institutional isomorphism

- Introduced by DiMaggio and Powell in (1991), explains how organizations in similar fields tend to become more alike over time as they adopt similar practices and structures to gain legitimacy.

BTC's evolution from a radical digital cash system to a widely recognized store of value: as Bitcoin gains mainstream acceptance, it adopts characteristics of traditional financial assets to align with regulatory standards and institutional practices, thereby diluting its original values.



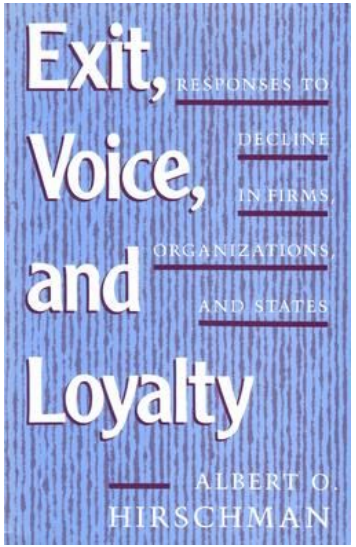
The New Institutionalism in Organizational Analysis (1991)

Change as consequence of voice or exit

"Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States"

Hirschmann presented a framework originally observing consumers' options in the context of deteriorating quality of goods and services: either exit or voice.

The framework has been applied to topics such as protest movements, migration, political parties, and interest groups, as well as to personal relationships.



Albert O. Hirschmann, 1970
ISBN 0-674-27660-4

Fully decentralized systems have characteristics that make them less prone to enshittification.

Their success in avoiding such degradation largely depends on the robustness of their governance models, the alignment of incentives, and the ability to scale effectively while maintaining user control and trust.

2

OPEN SOURCE

PUBLIC SOURCE AND OPEN SOURCE (Burns, 2015)

OPEN SOURCE
“The openness with people and code all wrapped up in one”

PUBLIC SOURCE
“everything that open source has minus all community side of things”

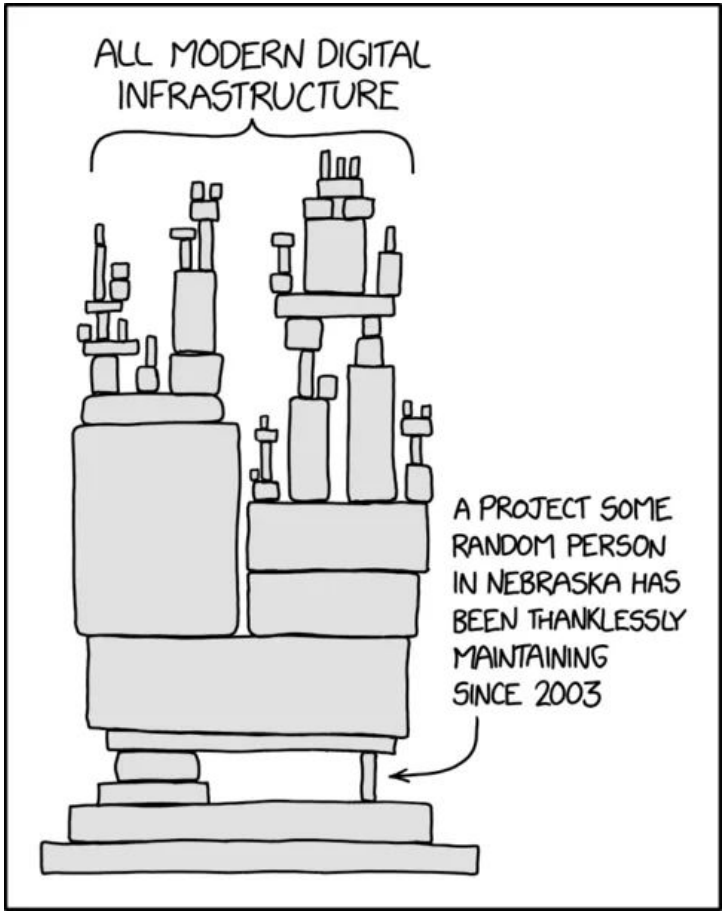
Example: try to upstream a patch to Android

🤣

Apple Public Source License

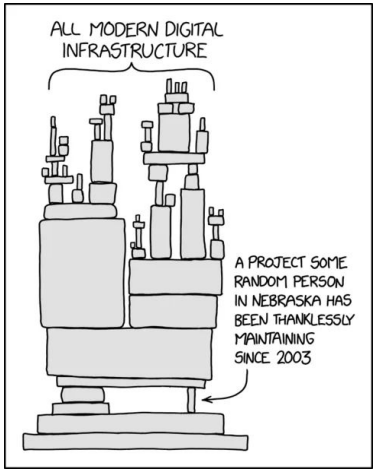
Author	Apple Inc.
Latest version	2.0
Published	August 6, 2003
SPDX identifier	APSL-1.0, APSL-1.1, APSL-1.2, APSL-2.0
Debian FSG compatible	No[1]
FSF approved	Yes (Version 2.0, not versions 1.0, 1.1 and 1.2)[2][3]
OSI approved	Yes
GPL compatible	No[2]
Copyleft	Partial[4]
Linking from code with a different licence	Yes[4]
Website	https://opensource.apple.com/apsl/

"software is eating the world" (Andreessen, 2011)


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Thanklessly maintained out of Nebraska

- XZ supply chain hack in 2024
- A backdoor was intentionally planted in XZ Utils, an open-source data compression utility available on almost all installations of Linux and other Unix-like operating systems.
- The xz-utils backdoor could have been the most serious software supply chain compromise since the SolarWinds Orion hack.



Missing incentives in Open source

"Developers are more likely to release closed-source software because it offers direct financial rewards, job security, and the potential for substantial personal gain. In contrast, open-source contributions are often seen as unpaid labor with minimal immediate benefits" (Murphy, 2024)

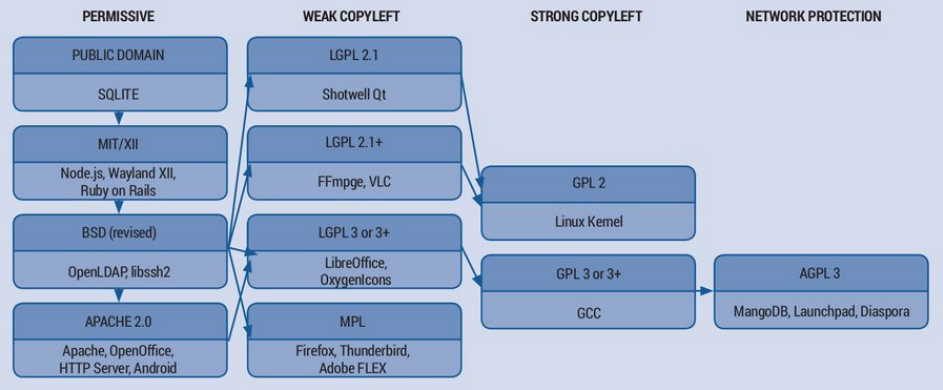
Monero CCS - Community Crowdfunding System (CCS)

Monero CCS is a positive example to solve the problem of “thankless maintenance from Nebraska”

https://ccs.getmonero.org/

“open source is eating software faster than software is eating the world”* (Jacks, 2022)

*** software with source code publicly available for inspection, use, and modification and is often created in a decentralized manner and distributed for free – appears in 96% of codebases (Synopsys 2023)**



2 links into the rabbit hole

- [John Winter Murphy: “Monero is Free and Open Source Software”]
- [/dev/lawyer blog]

In general, permissive open source licenses like MIT, BSD, and Apache say:

```
Do what you want with this software.
```

Copyleft licenses like MPL, GPL, and AGPL say:

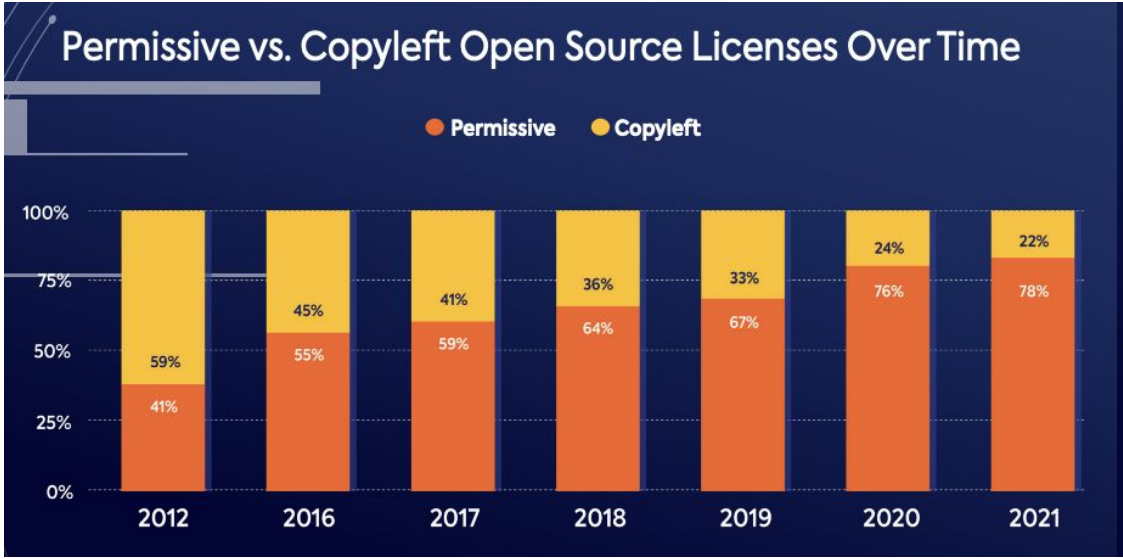
```
Do what you want with this software.

Share improvements and extensions you make
alike.
```

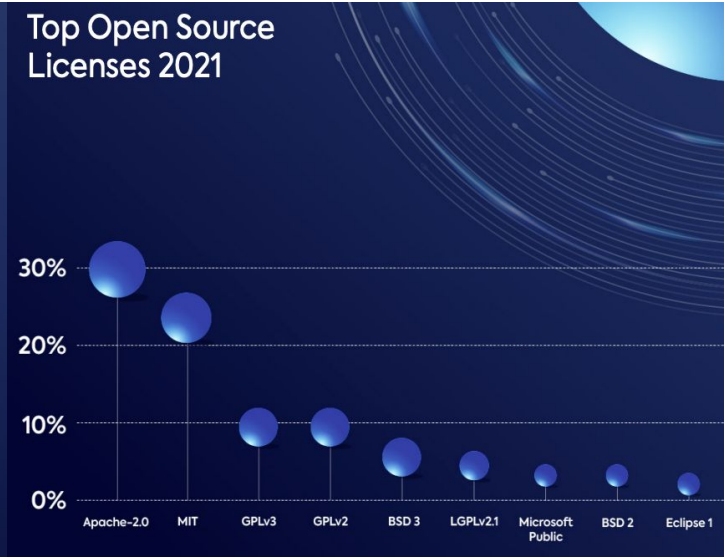
Commons Clause is a bolt-on “patch” to any open source license, permissive or copyleft. Generalizing a bit, Commons Clause appends:

```
+ But don't use it to compete with its
developer.
```

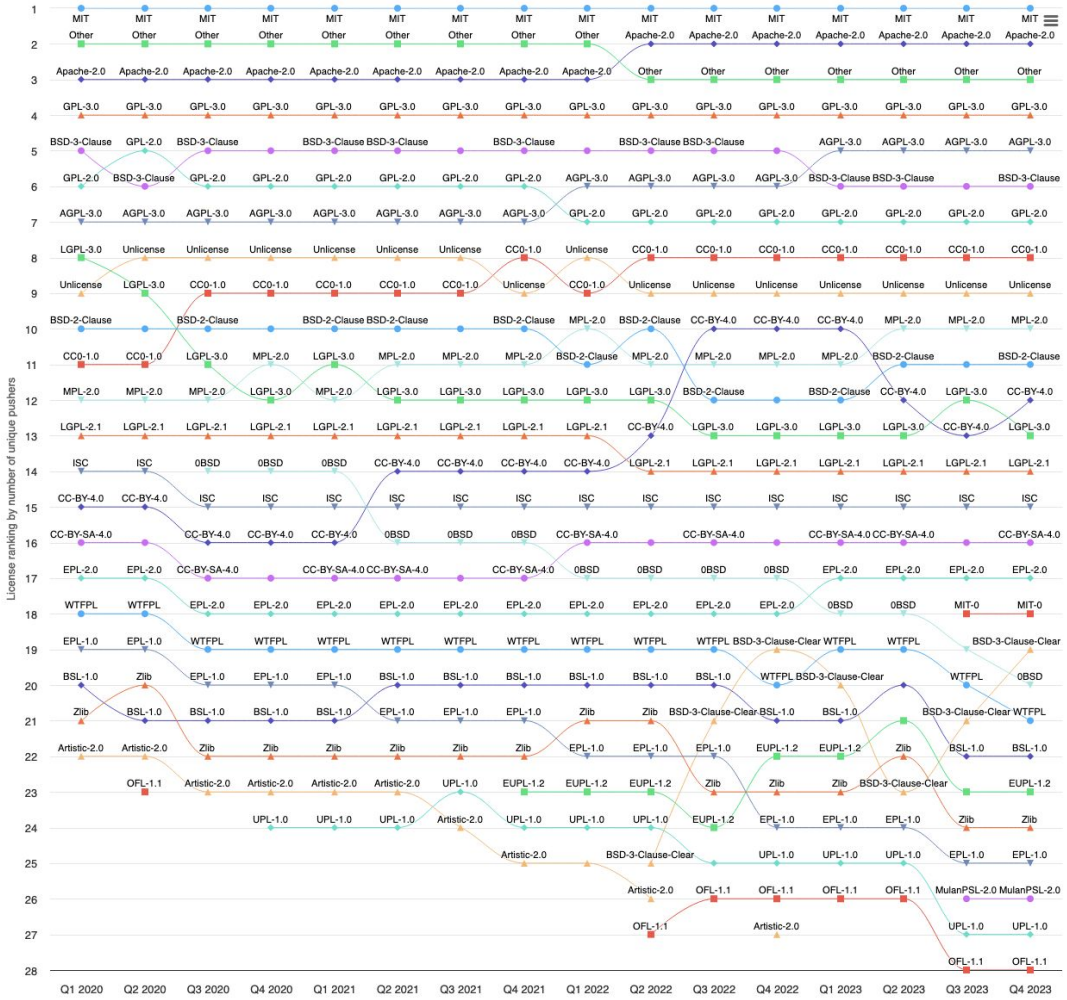
So “MIT with Commons Clause” says:

```
  Do what you want with this software.
+
+ But don't use it to compete with its
developer.
```



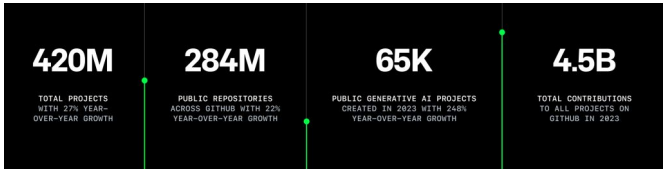


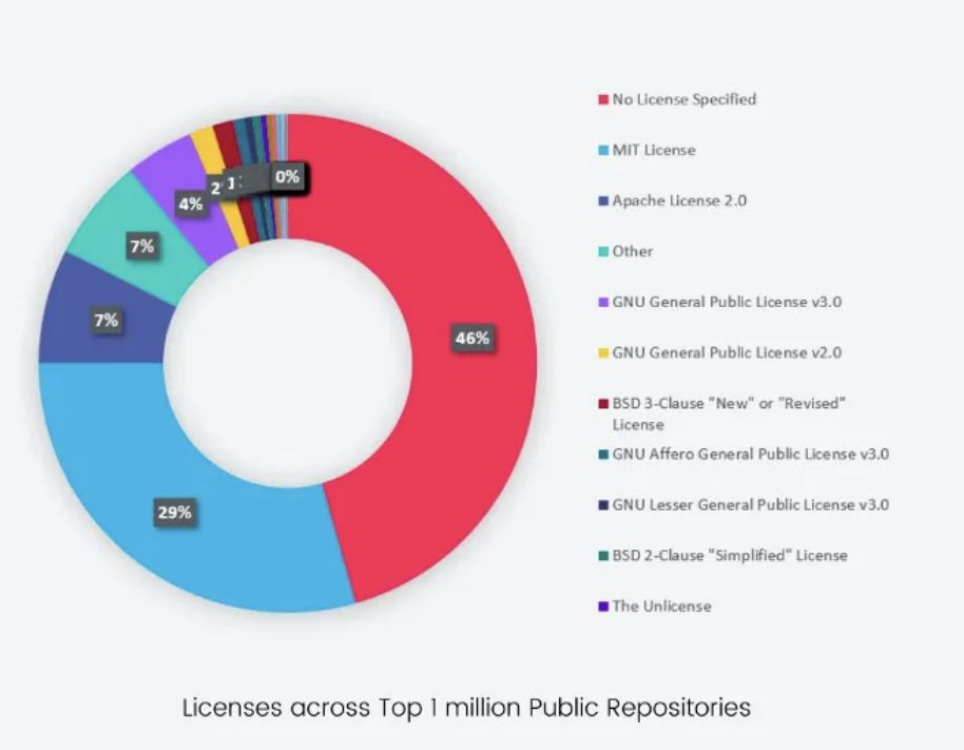
Permissive licenses dominate Open Source. Data from 2021.
Source: [WhiteSource, 2022]



https://innovationgraph.github.com/global-metrics/licenses

- MIT
- OTHER
- APACHE2
- GPL3
- BSD-3
- GPL2





Over Half of the GitHub Public Repositories are Not Open Source Licensed (data from 2020). Source: [openweaver]

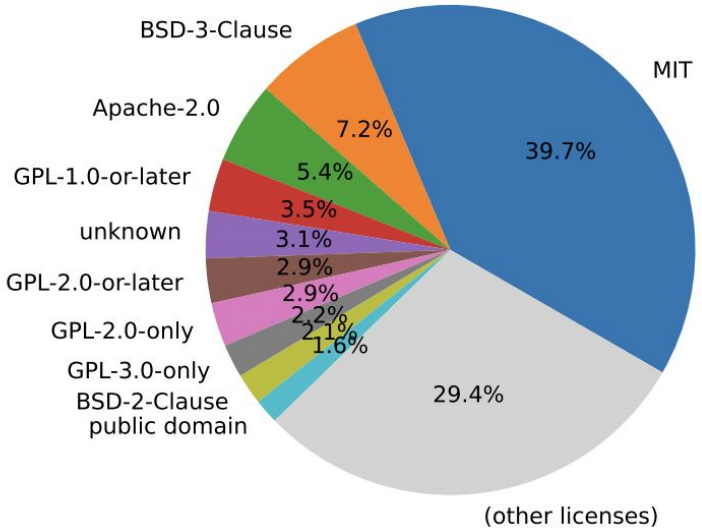


Figure 3: Top licenses in the corpus, as detected by ScanCode.

ABSTRACT

We introduce a large-scale dataset of the complete texts of free/open source software (FOSS) license variants. To assemble it we have collected from the Software Heritage archive—the largest publicly available archive of FOSS source code with accompanying development history—all versions of files whose names are commonly used to convey licensing terms to software users and developers.

The dataset consists of 6.5 million unique license files that can be used to conduct empirical studies on open source licensing, training of automated license classifiers, natural language processing (NLP) analyses of legal texts, as well as historical and phylogenetic studies on FOSS licensing.

Additional metadata about shipped license files are also provided, making the dataset ready to use in various contexts; they include: file length measures, detected MIME type, detected SPDX license (using ScanCode), example origin (e.g., GitHub repository), oldest public commit in which the license appeared.

The dataset is released as open data as an archive file containing all deduplicated license files, plus several portable CSV files for metadata, referencing files via cryptographic checksums.

Stefano Zacchiroli: A Large-scale Dataset of (Open Source) License Text Variants. 2022. Source: arxiv

Permissive open source licences are eating the commons faster than software is eating the world*

* data from 2022 shows that 78% of open source components have permissive licenses. (Source: mend)

Problem? YES.

We need more open systems, because we want to be able to verify them.

Hence we need less black boxes.

Monero is under a permissive License (MIT)

We had a lot of malicious fork attempts

Let's get eyes on the licensing discussion! [LMDB] (2017, Reddit)

noot's XMR-ETH atomic swaps CCS proposal finally moved to funding stage after licensing debate (2022, monero.observer)

Software Licensing OR "believe in one less god" (2022, Reddit)

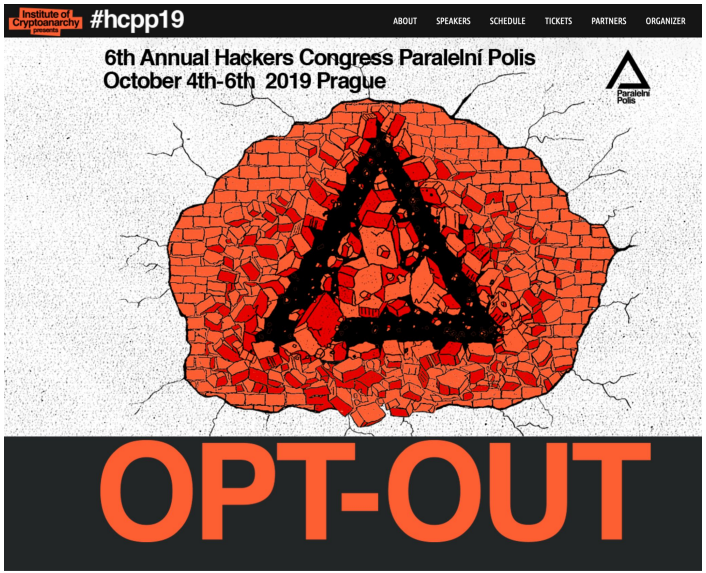
3

VERIFY ALL THINGS

Monero is verifiable software!

Monero reproducible builds

https://github.com/monero-project/monero/issues/2641

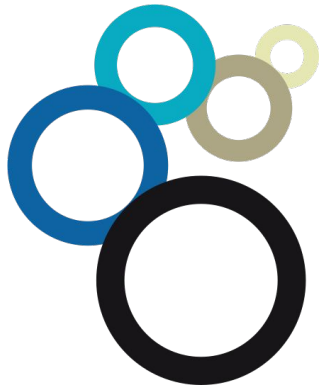


The past, present and future of Opt-Out with open and libre hardware #HCPP19

https://www.youtube.com/watch?v=jWRZfbWUszo

FREE, PUBLIC, OPEN SOURCE THINGS

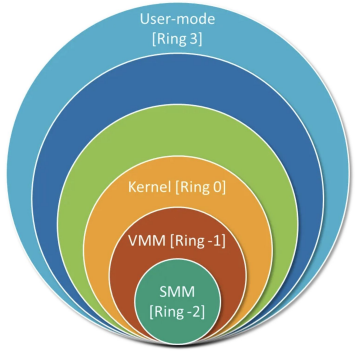
- Software
- Content
- Data
- Hardware*



* Further reading: Do I need to patent before open-sourcing hardware?; Towards open source patents (OSHWA certification database); Licensing Open Source Hardware (Michael Weinberg)

THE PROBLEM

- Many proprietary systems are black boxes, preventing users from verifying their functionality and security.
- Open source software “allows anyone to inspect, modify, and enhance the code” (potentially)
- “Open” systems are not necessarily verifiable



The protection rings mechanism. The lower the ring number, the more privileged the ring.

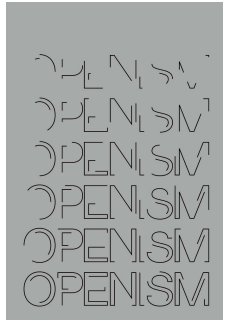
OPEN CATEGORIES

- Open Standards
- Open Access
- Open Design
- Open Hardware
- Open Education
- Open Government

}

OpenAI

The term “open” is very inflationary (see: Openwashing)



“Open Source is Insufficient to Solve Trust Problems in Hardware”

Bunnie Huang at 36C3

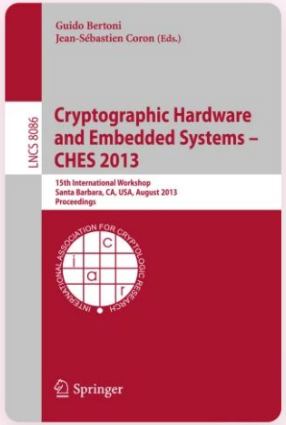
HARDWARE TROJANS

Conference paper

Stealthy Dopant-Level Hardware Trojans

Conference paper

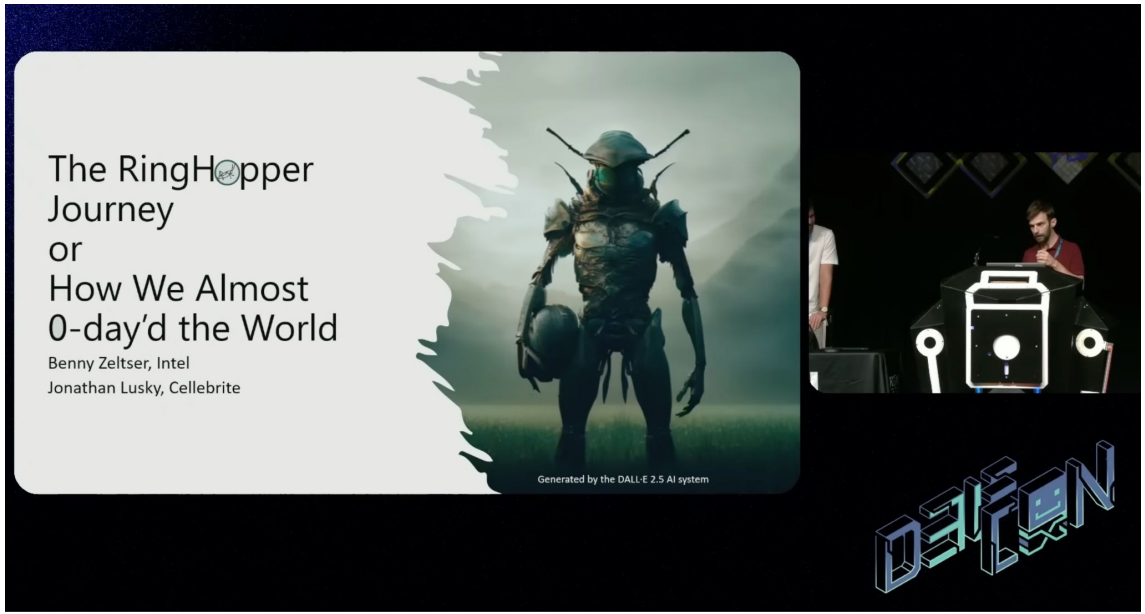
pp 197–214 | Cite this conference paper



Cryptographic Hardware and Embedded Systems – CHES 2013

(CHES 2013)

UEFI VULNERABILITIES



RingHopper, presented at DEF CON 31

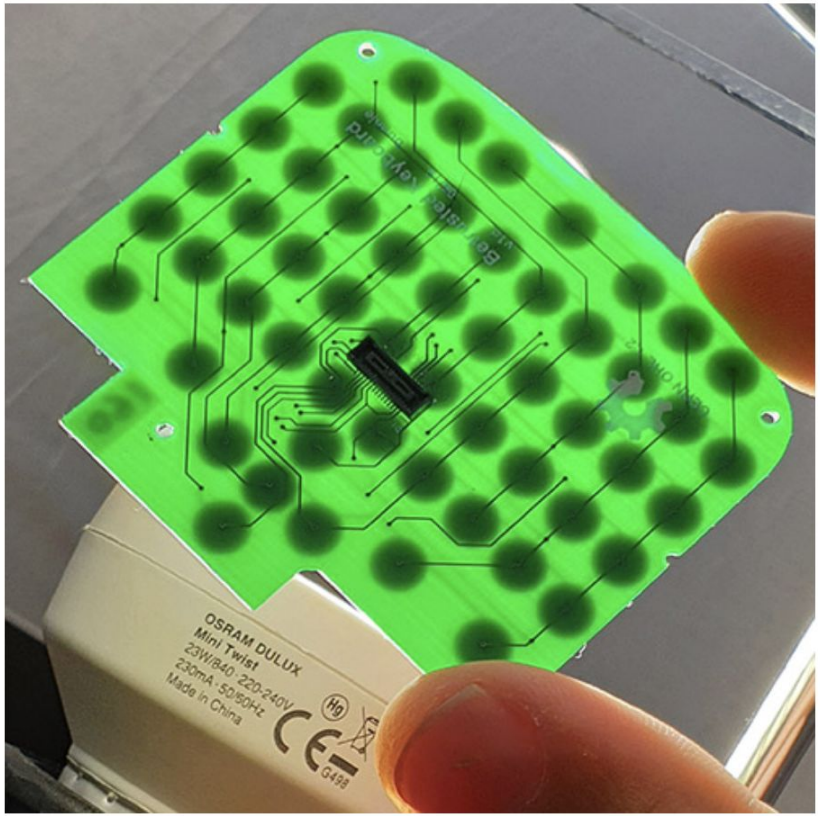
VERIFICATION?

- Modern **hardware** cannot be verified. The chances of backdoors or implants are given.
- **Firmware** & **device drivers** have binary blobs and microcode, which you cannot use without trusting suppliers.
- A huge problem are mobile phones (especially the modems), as they are only available in binary and proprietary form. Verification is only possible through extensive reverse engineering. Read the replicant wiki for more information.

Replicant

Verifiable I/O

For example, the input surface for Betrusted is a physical keyboard. Physical keyboards have the benefit of being made of nothing but switches and wires, and are thus trivial to verify.



Decentralized verificiation

- Current technology is very hard (or impossible) to verify.
- We still need to find methods to reverse engineer or verify processes in these black boxes.

In order not to have to reverse,
we need less black boxes in existence.

Linus's Law asserts that *given enough eyeballs, all bugs are shallow*, but we don't really know how many eyeballs are "enough." However, don't underestimate the number. Software is very often reviewed by more people than you might imagine. The original developer or developers obviously know the code that they've written. However, open source is often a group effort, so the longer code is open, the more software developers end up seeing it. A developer must review major portions of a project's code because they must learn a codebase to write new features for it.

Understanding Linus's Law for open source security

4

Nurturing decentralization and the commons (conclusion)

- **Platforms and products decay over time.**
- **Values need to be constantly re-validated.**

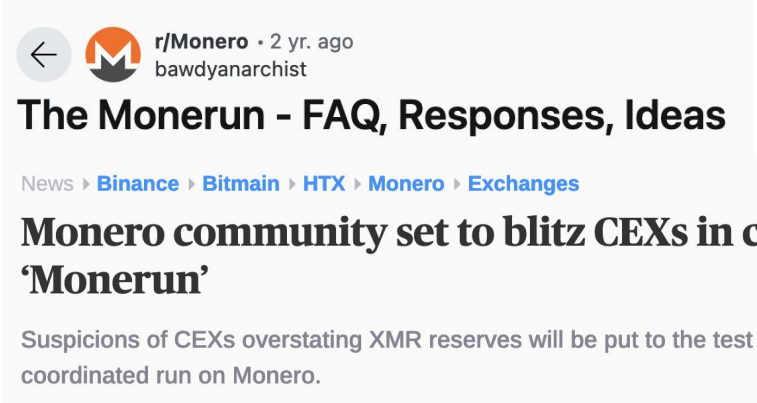
- **Open source is enshittified, and “open” does not necessarily mean “verifiable”, which is a problem for cypherpunk values.**

- **Technical literacy and reverse engineering help us in creating “verifiable things”, but there are strong limitations (see: binary blobs, hardware).**

- **Monero is verifiable software that aligns with cypherpunk values.**

The Monero Community is a great example for a cypherpunk culture with decentralized coordination capability. The Monerun was an amazing demonstration of decentralized verification of centralized exchanges.

https://www.reddit.com/r/Monero/comments/u57qky/the_monerun_faq_responses_ideas/



“Decentralisation is a process, and should be constantly challenged.” (decentral.community, 2019)