Lecture 1
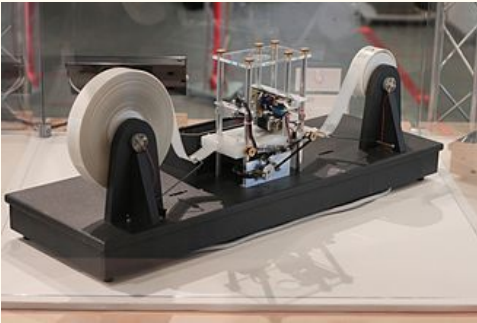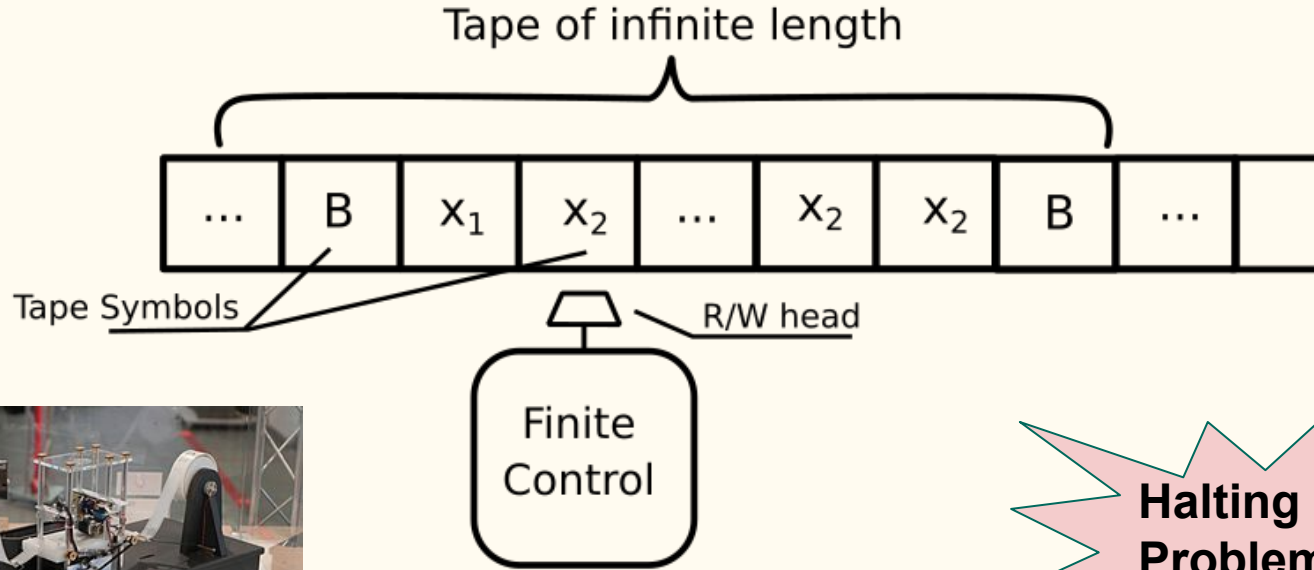
—

Blockchain Basics and Development

A history of computing and Ethereum

What is 3 in Web3?

[1939] Turing machine / Turing Completeness

Tape of infinite length

Tape Symbols

R/W head

Finite Control

Halting Problem!

Turing - The cost of memory

1TB Crucial P3 SSD M.2 2280
PCIe 3.0 x4 3D-NAND QLC

[1951] UNIVAC I - computers commercially available

Filled a room

Available only to government and universities

Maintenance was extremely difficult and niche

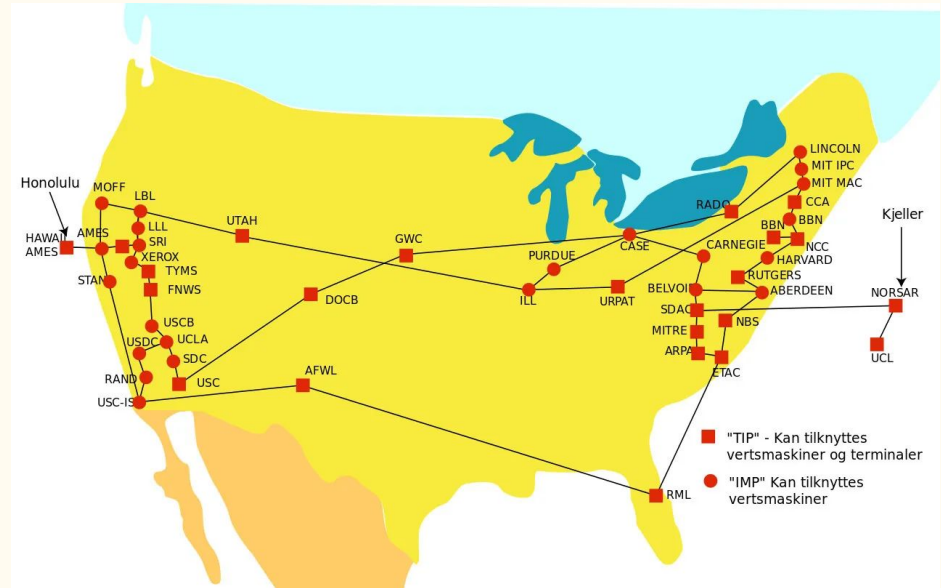# [1952] IBM and PACT - birth of open source

IBM Type 701

Composed of 11 "compact" units

Project for the Advancement of Coding Techniques (PACT)

[1960s - 1983] Birth of the Internet

ARPANET —> TCP/IP

[1991] Web1 - Static age of information

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
    Pointers to the world's online information, subjects , W3 servers, etc.
Help
    on the browser you are using
Software Products
    A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
    Details of protocols, formats, program internals etc
Bibliography
    Paper documentation on W3 and references.
People
    A list of some people involved in the project.
History
    A summary of the history of the project.
How can I help ?
    If you would like to support the web..
Getting code
    Getting the code by anonymous FTP , etc.

Cyberpunks Movement - Secure, Anonymous, Independent

❖ Many attempts to create a digital currency and break free from traditional banking
  ➢ eCash by David Chaum in 1983
  ➢ HashCash, eGold, BitCash

❖ Lacked awareness, suffered from attacks, used for dark web activities

[2000s] Web2 - Dynamic age of interaction

Websites able to respond to user input

Storage of user information (risk!)

Users now interact with each other and leave reviews (asymmetrical information)

[2008] Web 3 - Age of decentralization

Wallet addresses instead of user information

Extreme transparency without identity

No central authority, truth must be agreed upon - consensus

[2013] Ethereum - A Turing Complete State Machine

**Ethereum World State
Merkle Patricia Trie**

EOA
Smart contracts
Address

To

Balances, Nonce, Variables,
address pointers, gas limits

……

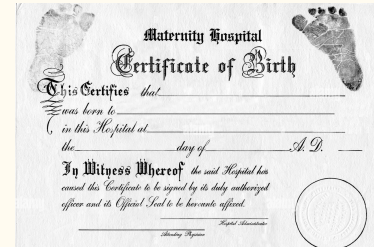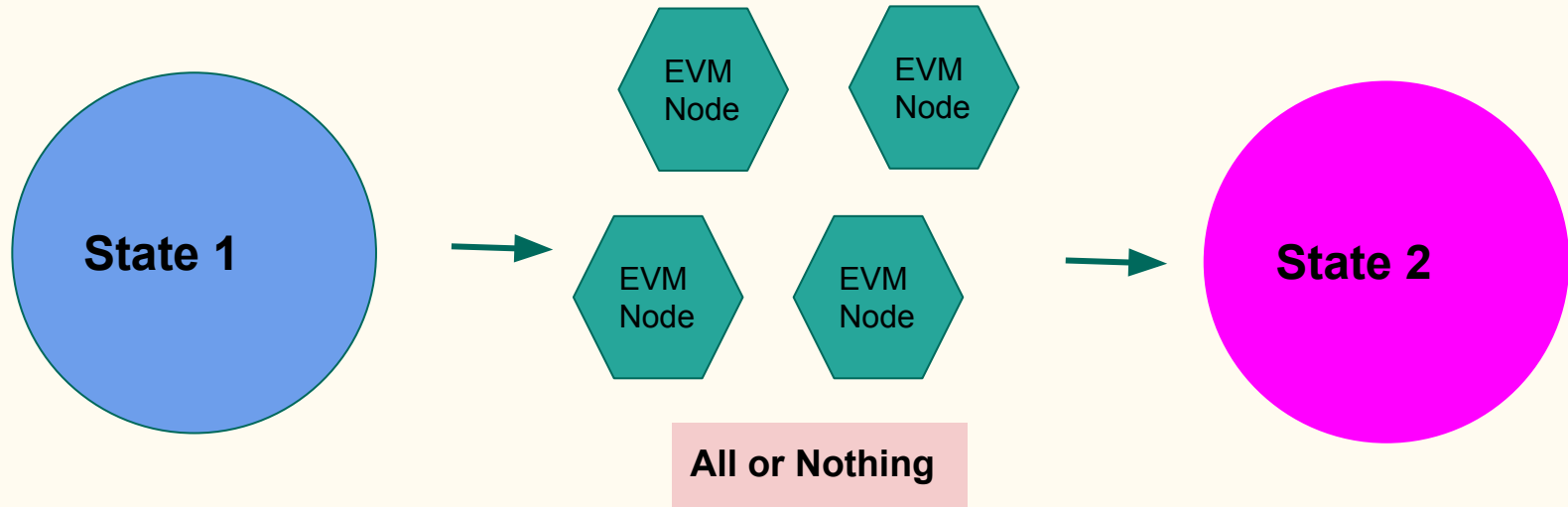**Externally Owned
Accounts**
- No Code, no data
- Public/private keys
- Hardware, software

Smart Contracts
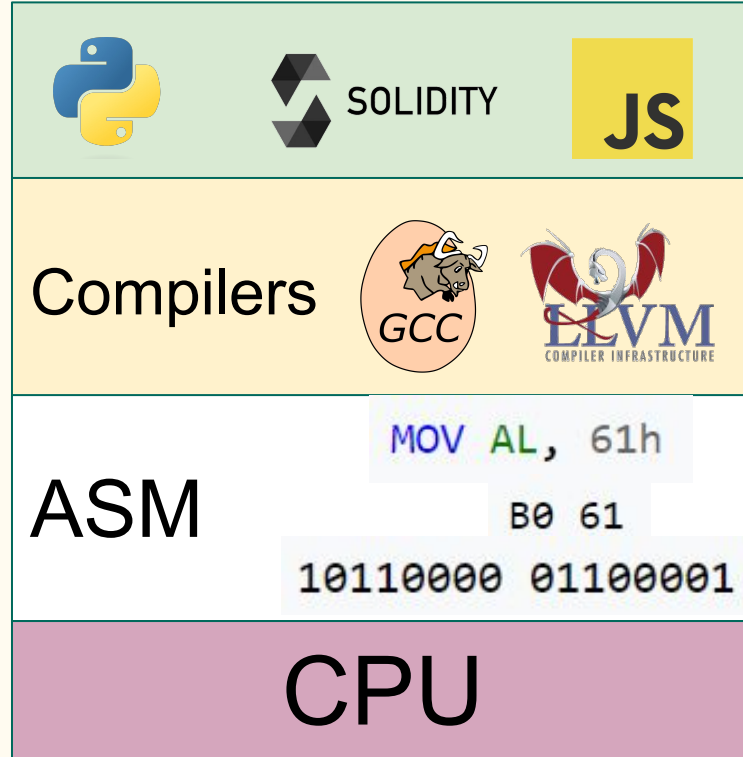- Hash of code and data
storage
- Needs a sender address

Ethereum - A Turing Complete State Machine

Turing Machines
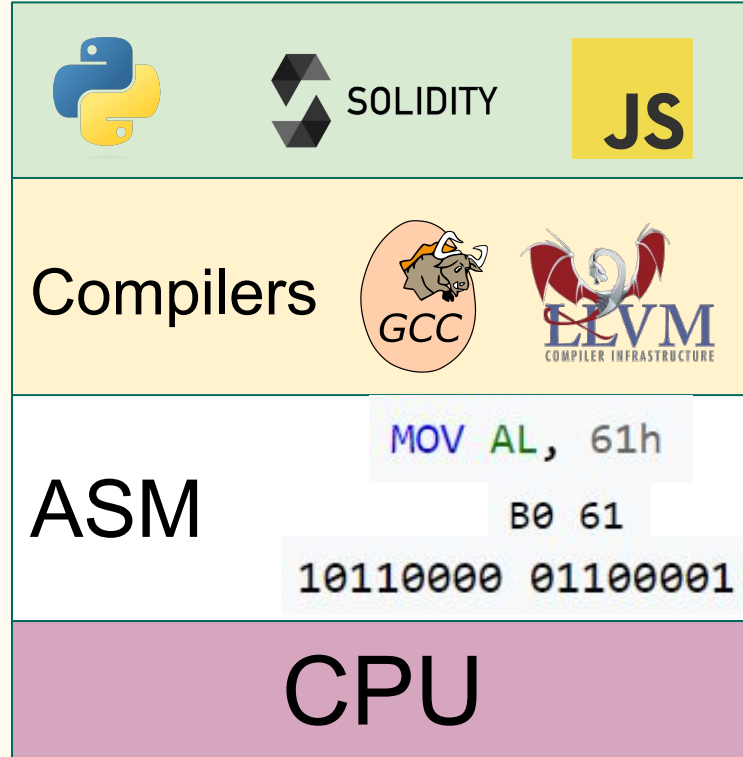## A history and A comparison

Web 2 vs Web 3 Architecture

Human readable - "High Level"

Translation program:
Bytecode -VM
Machine Code - Binary
ASM - Instructions

Machine Language - "Low Level"

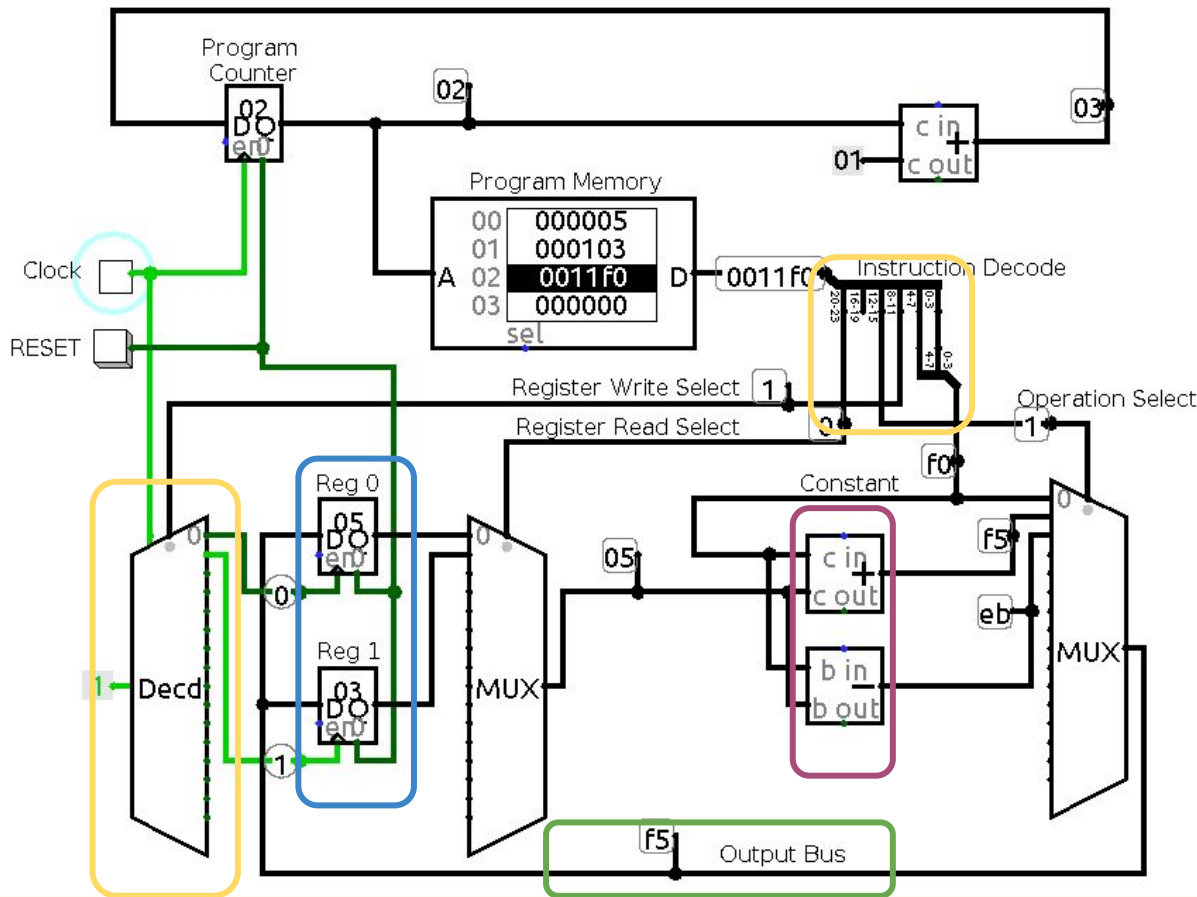A Turing Complete, Finite State Machine

Web 2 vs Web 3 Architecture


```
 var a;
 a = 1+1

malloc 256;
add 1 1
write a 2

01101 256
00100 0001 0001
10001 0x456 0010
```
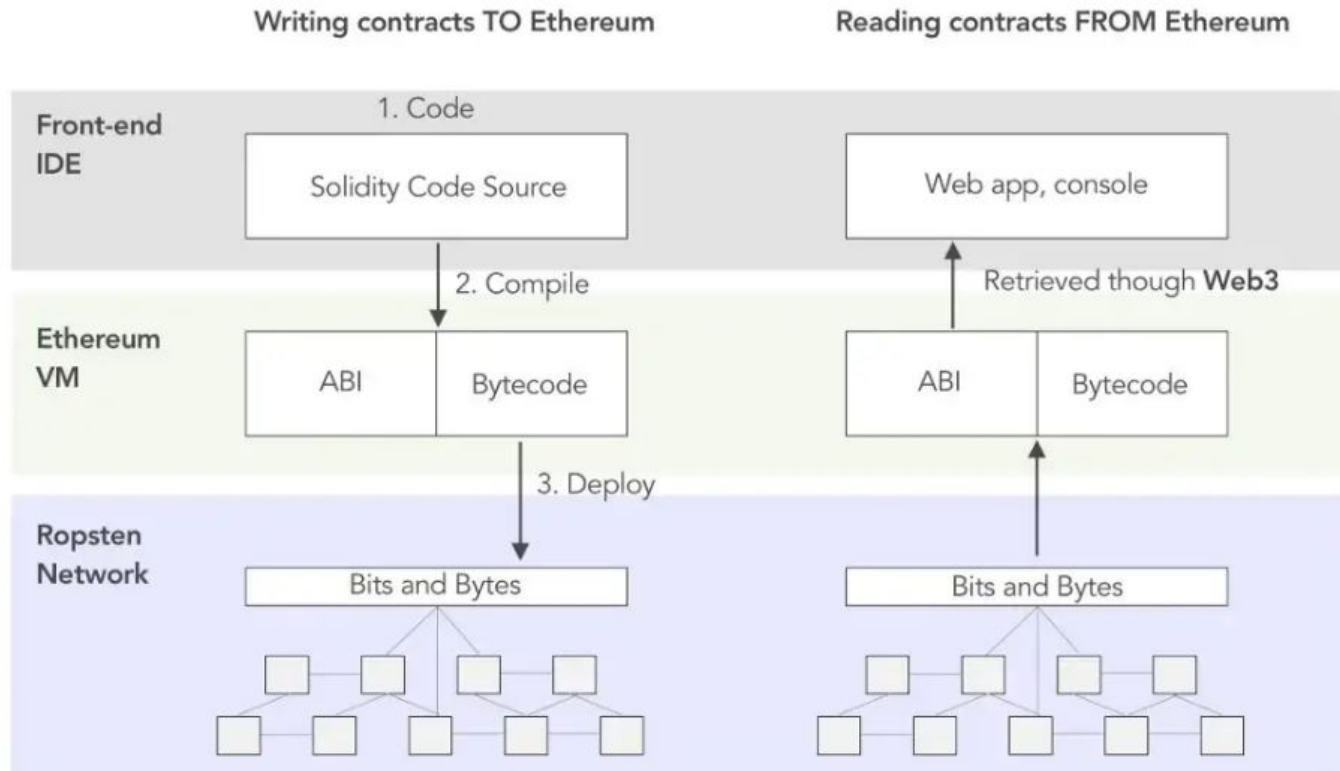
Web 2 vs Web 3 Architecture

Decode Instructions into opcode and data

Registers to hold **program** essentials: Data, loops state, pointers

Algorithmic Logic Unit

Ram read write, towards more permanent storage. Indexed by **Addresses**

Web 2 vs Web 3 Architecture

Writing contracts TO Ethereum — Reading contracts FROM Ethereum

Front-end IDE: 1. Code — Solidity Code Source / Web app, console

2. Compile / Retrieved though **Web3**

Ethereum VM: ABI / Bytecode — ABI / Bytecode

3. Deploy

Ropsten Network: Bits and Bytes — Bits and Bytes

Source: https://hackernoon.com/ethernaut-lvl-0-walkthrough-abis-web3-and-how-to-abuse-them-d92a8842d71b

Web 2 vs Web 3 Architecture
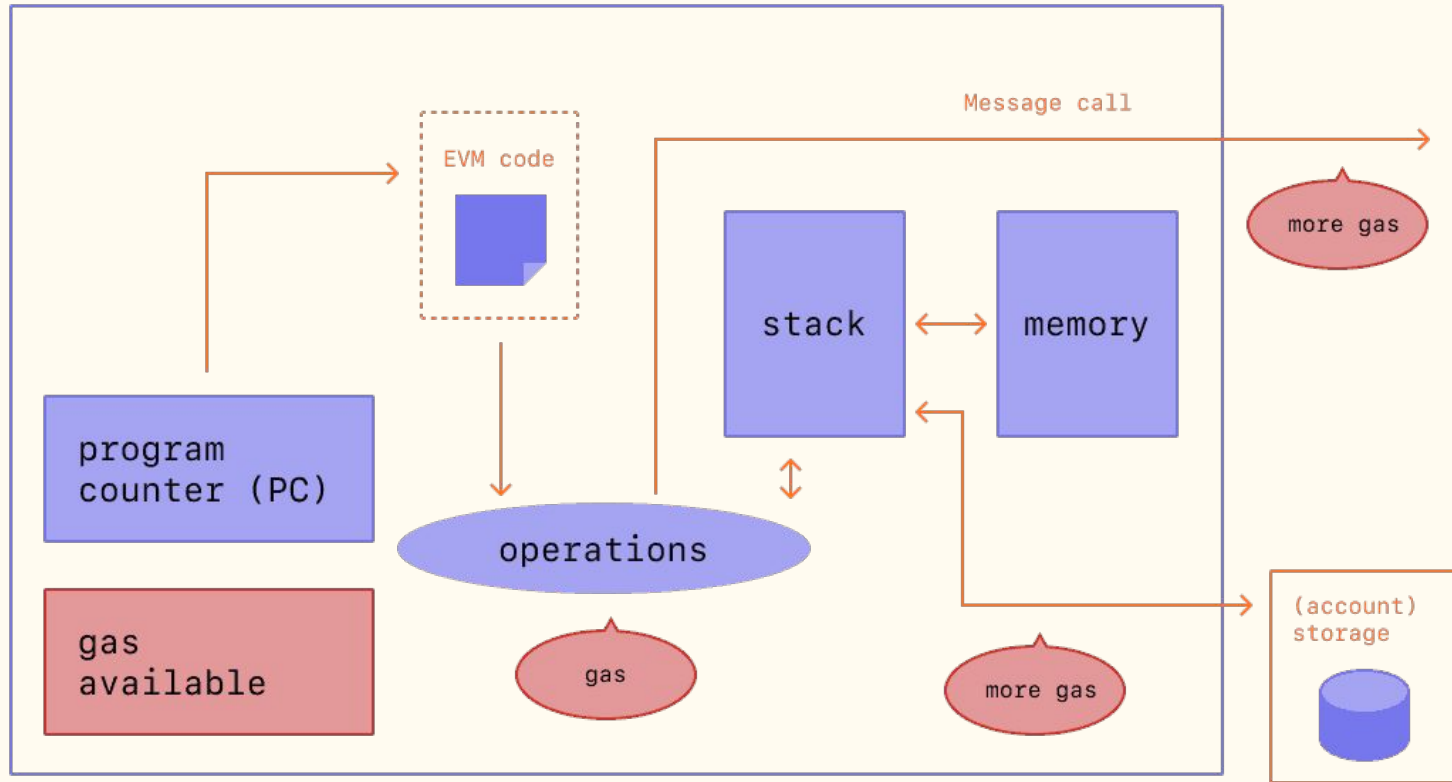
Open Source

The principle that inspired Decentralization

Free Software Movement

4 Fundamental Freedoms

Purpose Freedom to run the program as you wish, for any purpose.	**Knowledge** Freedom to study and modify the program.
Solidarity Freedom to distribute your creations to help others	**Community** Freedom to redistribute changes and improvements for the benefit of the community

Battle of the Copies - Left vs Right

Open Source Licensing - The corporate strikes back

Permissive

Copy Left

Weak

Strong

- Do what you want
- You can copyright your version
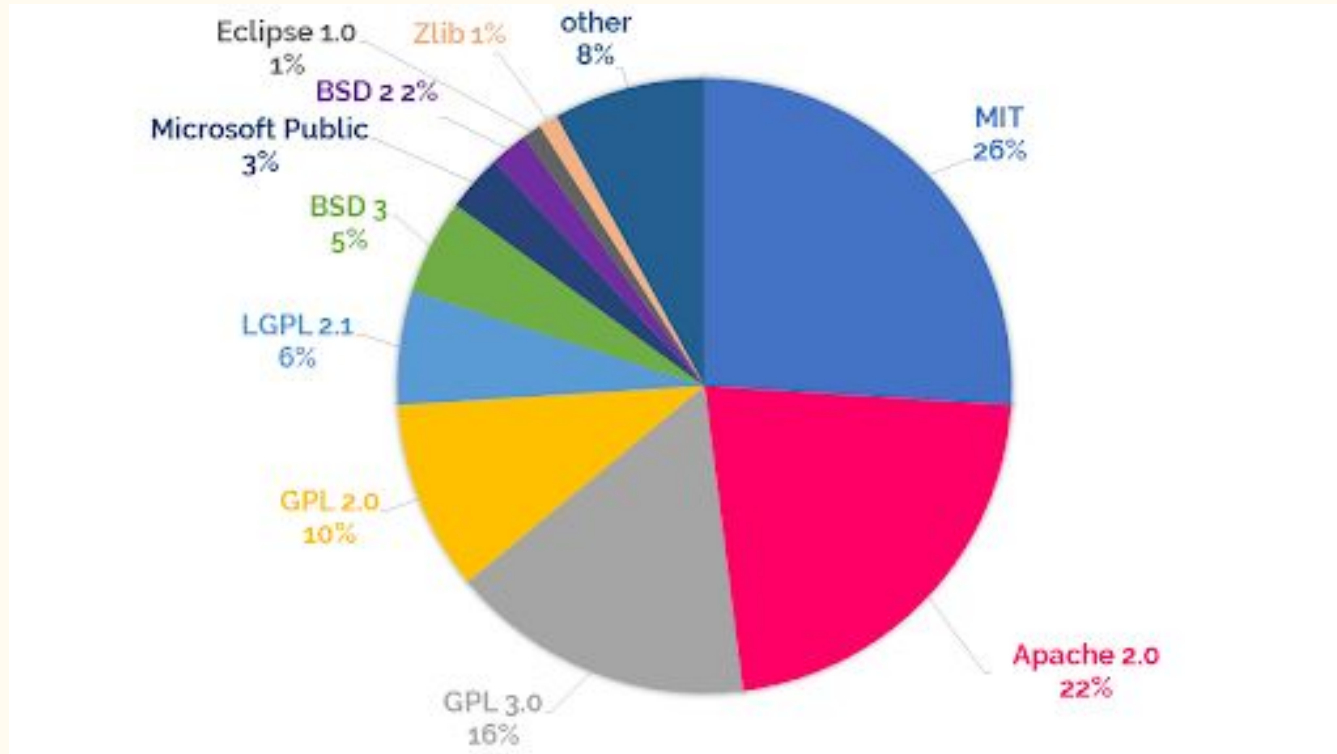- Don't sue me
- No marketing? (BSD3)
- Can withdraw (Apache2)

- Must show source code of the original or direct modification
- your own code can be proprietary (use original as library)

- Must show source code!
- If you use this code, your code must also be show
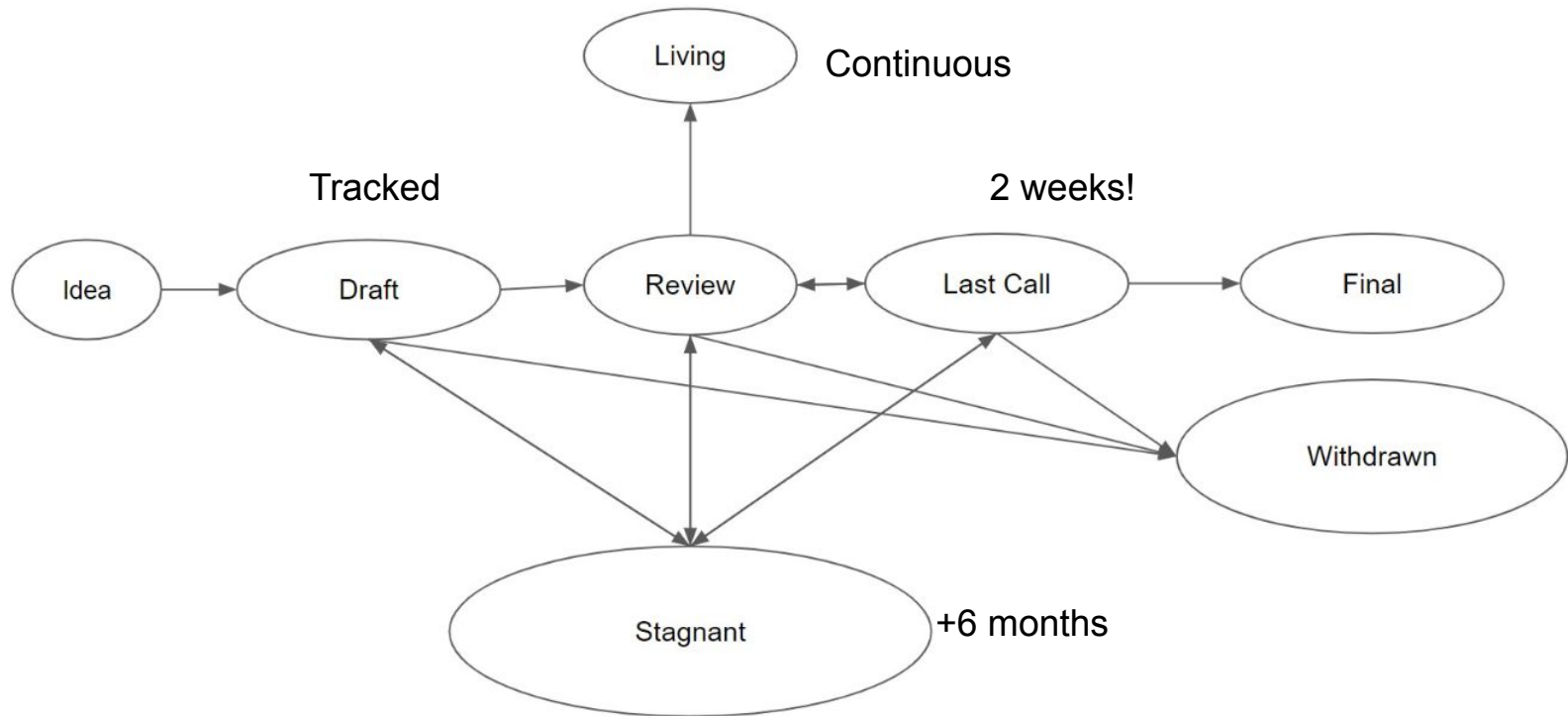- Known as 'viral'

Open Source Licensing - current distribution
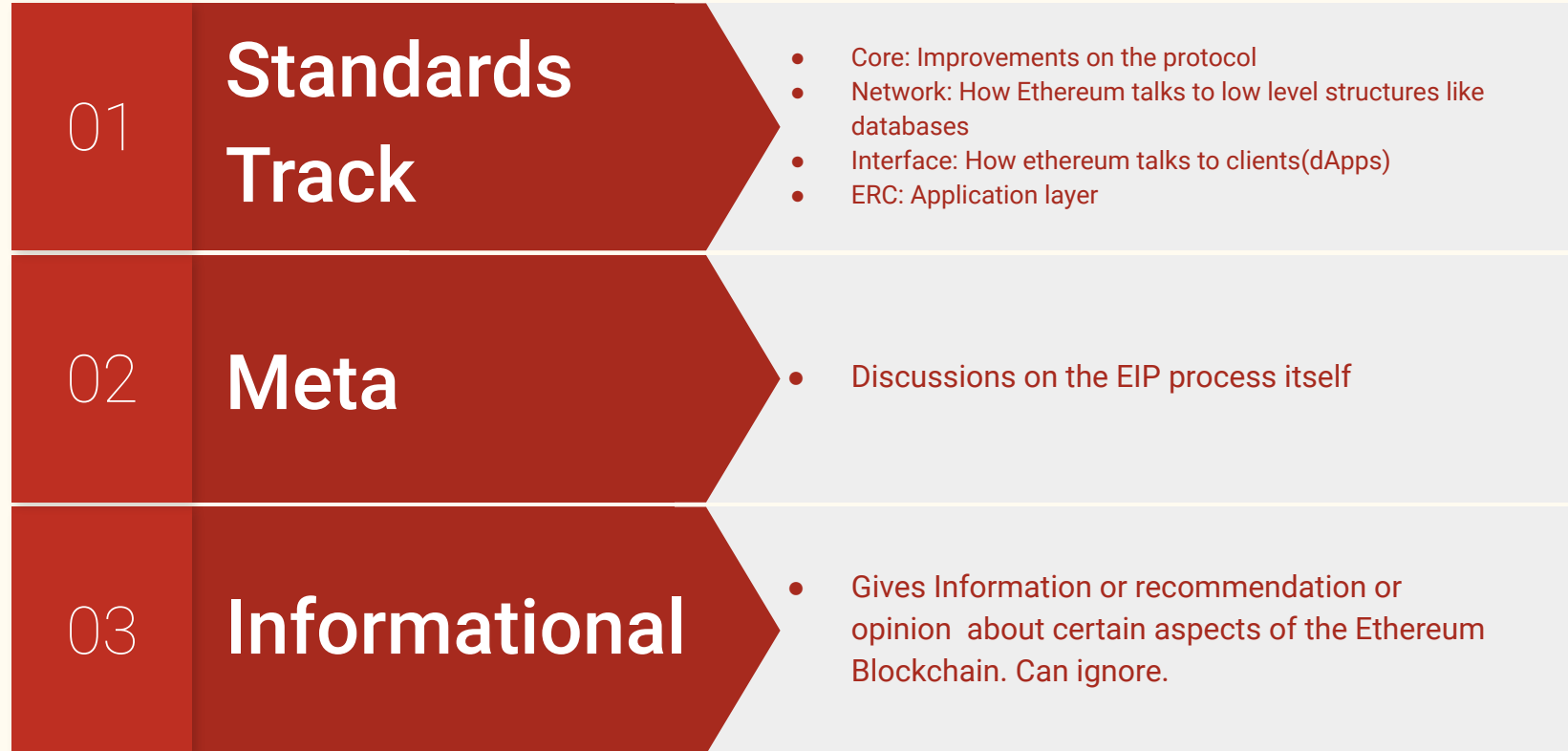
Check out our class Github!

https://github.com/Dauphine-Digital-Economics

How to be an open source Contributor - Ethereum Improvement Proposals

How to be an open source Contributor - Ethereum Improvement Proposals

01 **Standards Track**

- Core: Improvements on the protocol
- Network: How Ethereum talks to low level structures like databases
- Interface: How ethereum talks to clients(dApps)
- ERC: Application layer

02 **Meta**

- Discussions on the EIP process itself

03 **Informational**

- Gives Information or recommendation or opinion about certain aspects of the Ethereum Blockchain. Can ignore.

List of important EIP standards

ERC20 - Token standard

ERC721 - NFT Standard

ERC1155 - Multitoken Standard

ERC2981 - NFT Royalty Standard

ERC4626 - Tokenized Vaults

https://eips.ethereum.org/erc