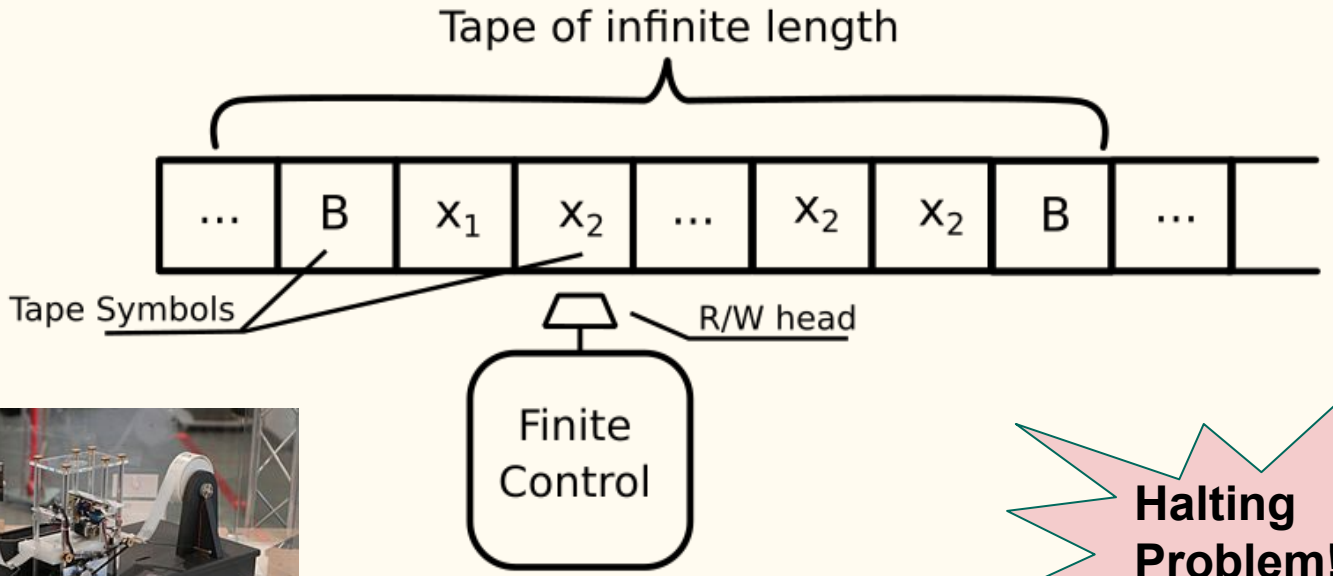
Lecture 1

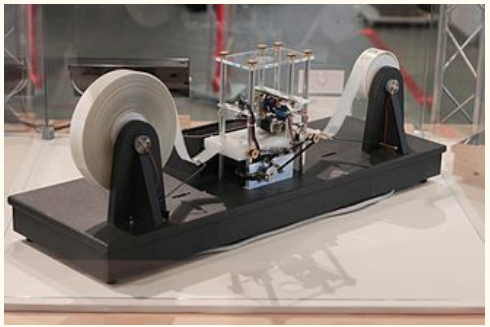
History and Architecture of Blockchain

A history of computing and Ethereum

What is 3 in Web3?

[1939] Turing machine / Turing Completeness





1. Read or Write
2. Perform calculation, understand state
3. Decide to move left or right

Halting Problem!

Source: https://iq.opengenus.org/general-introduction-to-turing-machine/

Computational finance - The cost of memory and computation power

Static, private memory

amazon web services

OVH.com

XaaS, on cloud

Decentralized ledger

[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

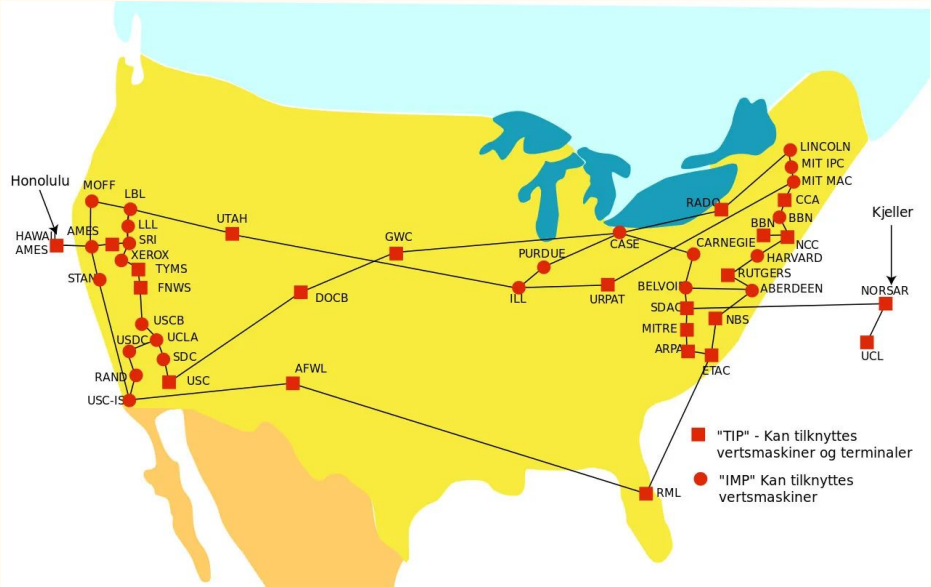
Composed of 11 "compact" units
$12,000 monthly rental
1 william tube = 1kb

Universities band together against these large corporations

Project for the Advancement of Coding Techniques (PACT)

[1960s - 1983] Birth of the Internet

ARPANET —> TCP/IP



Bonus Point

With the advent of the Internet, users are able to access shared knowledge. This triggered the field of distributed computing.

In distributed computing, managing the state of global variables becomes a central focus point. Who can access and when are changes accounted for?

Q: What is the equivalent of this problem in finance?

Cypherpunks Movement - Secure, Anonymous, Independent

- Central tenets of Cypherpunks:
  - Strong encryption = digital freedom
  - Governments and corporations shouldn't be able to easily spy on people
  - Privacy should be protected by code, not laws

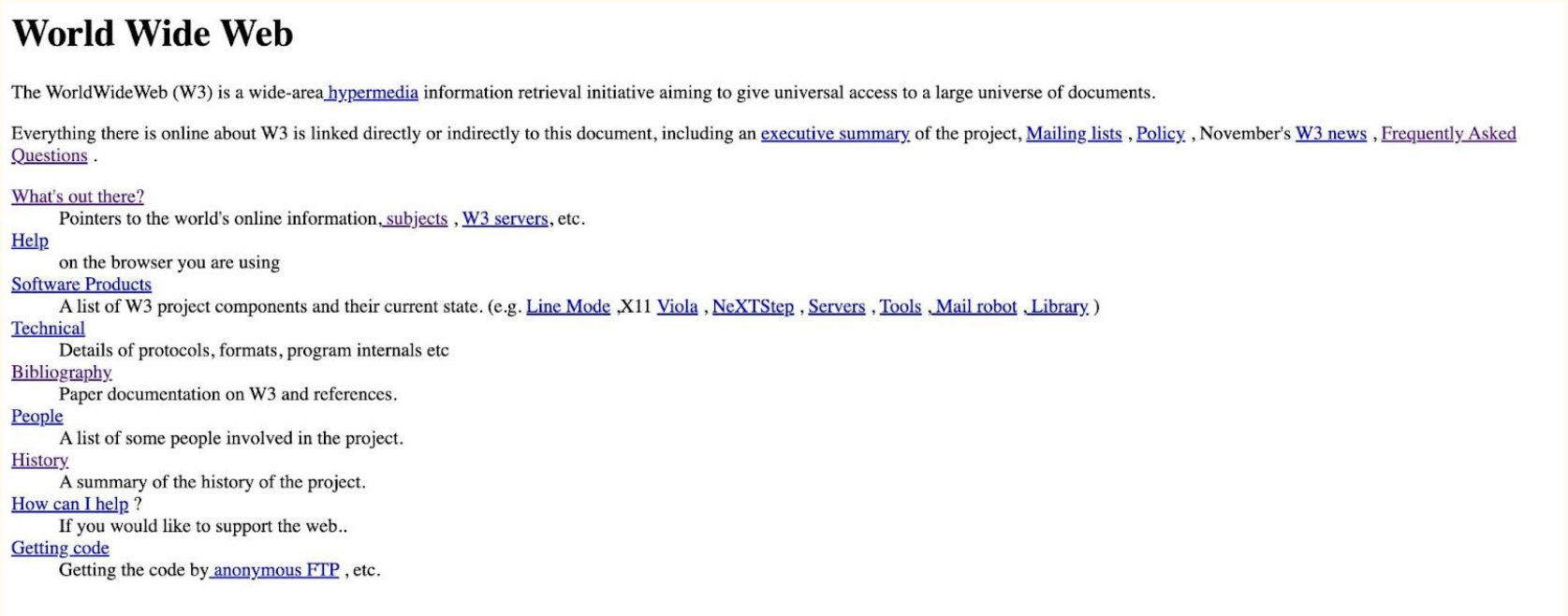
- Many attempts to create a digital currency and break free from traditional banking
- Lacked awareness, suffered from attacks, used for dark web activities

DIGI CASH®

1989 - David Chaum, DigiCash
Blind signature transaction
Limited adoption, bankrupt 1998

1989 - Dai Wei, b-Money
Democratisation of transaction verification
Never implemented, no community (miners)

[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.

[2000s] Web2 - Dynamic age of interaction

Websites able to respond to user input

Storage of user information/identity.

Large conglomerates promise privacy.

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

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

[2008] Web 3 - Age of decentralization

2008 Financial Crisis shakes trust in the establishment

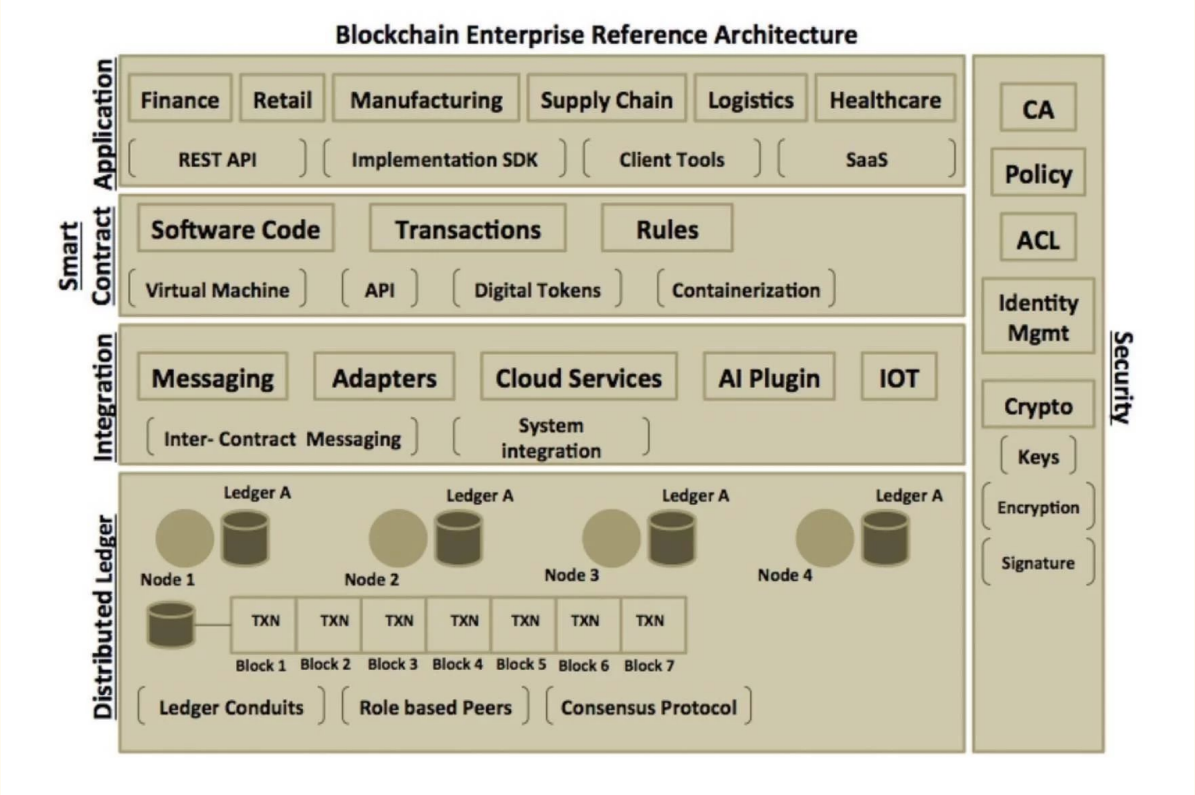
Wallet addresses instead of user information

Flipped ideology - transparency without identity

No central authority, truth must be agreed upon - consensus

What is blockchain technology?
Anonymous computers voting on the truth
This truth is transparently recorded in block format

Blockchain architectural stack



Use cases: Digital Euro, Space Supply Chain

Network Simulation via Smart Contracts

Oracles, introducing external data

Network effects and consensus

Source: https://navveenbalani.dev/index.php/articles/blockchain-reference-architecture/

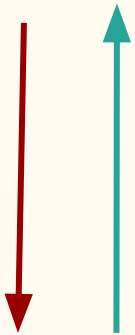
Open Source Communities

Github technicalities and evaluation

Open Source Orgs

Author - Original creator of project
Owner - Highest admin. Can be author or someone else
Maintainers - Core dev group, responsible for project vision and roadmap. Sometimes divided into committees.

Keep the community healthy and engaged.
Align on the vision and roadmap
Approve contributors' work
Manage commercialization - Sponsors, Enterprise maintenance



Creates new features, bug fixes.
Provides feedback, UX

Contributors - Adds technical or material content to the project.
Community Member - Uses the software, provides feedback.

Types of Contributors

Technical	Content	Community
New comers: - Good first issue - Code cleanliness, linting **Seasoned devs:** - Propose new features - Roadmap assistance - Bug fixes - PR review support - Mentorship	- Translations - Project Documentation - Tutorials - Learning materials (eg. Quizzes)	**Ambassadors:** - Host events to grow community. - Measure engagement - Pass issues to devs to resolve **Platform Managers:** - Social media presence - Resolve conflict, marketing

Open Source Metrics

Developer Metrics

Monthly Active Developers - How many new github accounts contributing?

Full time vs part time vs one time devs

Dev localisation - some countries / cities more active than others

Repo Metrics

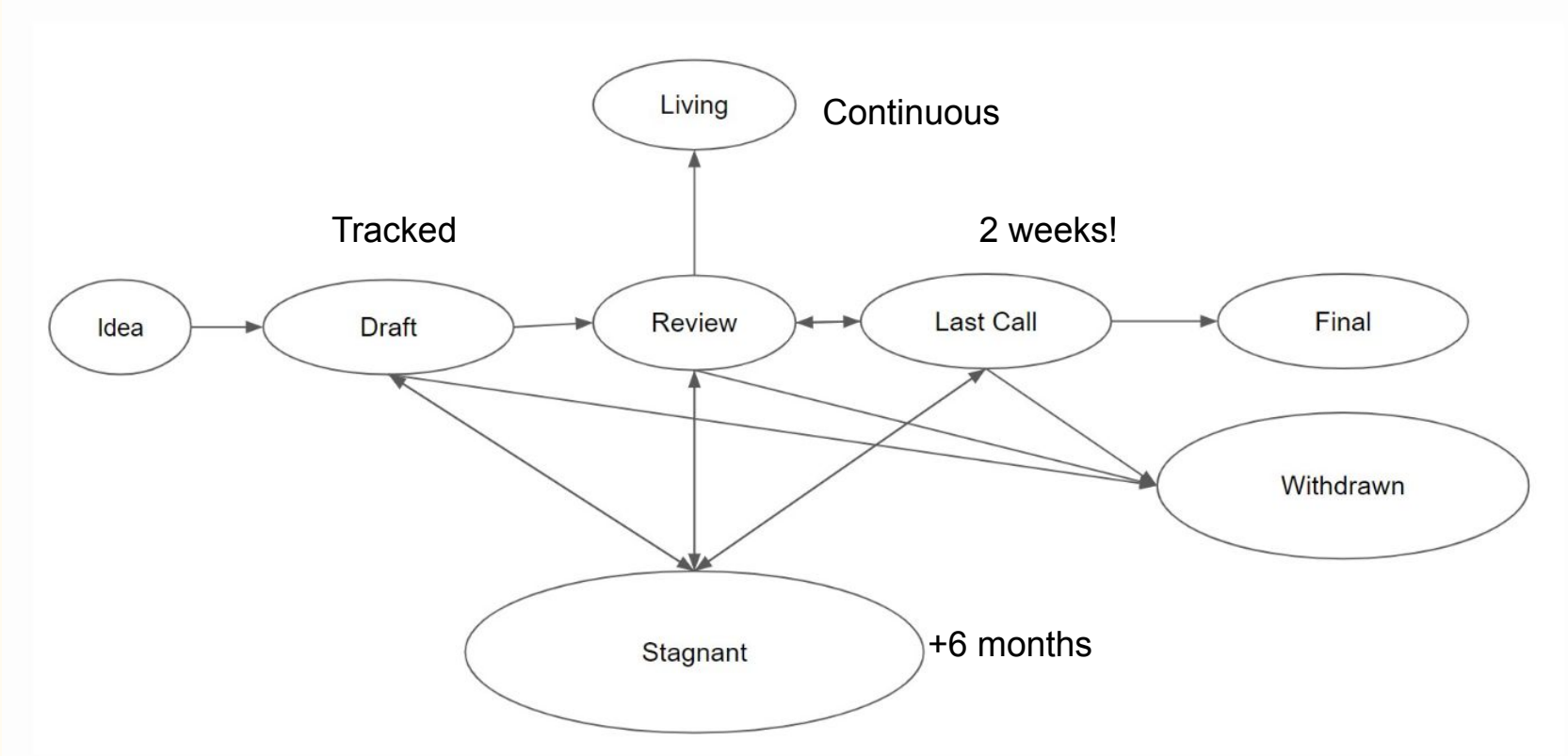
# of PRs, issues - open and close rates

# of Stars and Forks - level of interest

Sponsors - financial health

Time between releases and bug fixes - operational health

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

ERC1559 - Fee Market Change

ERC4824 - DAO Standard

https://eips.ethereum.org/erc