

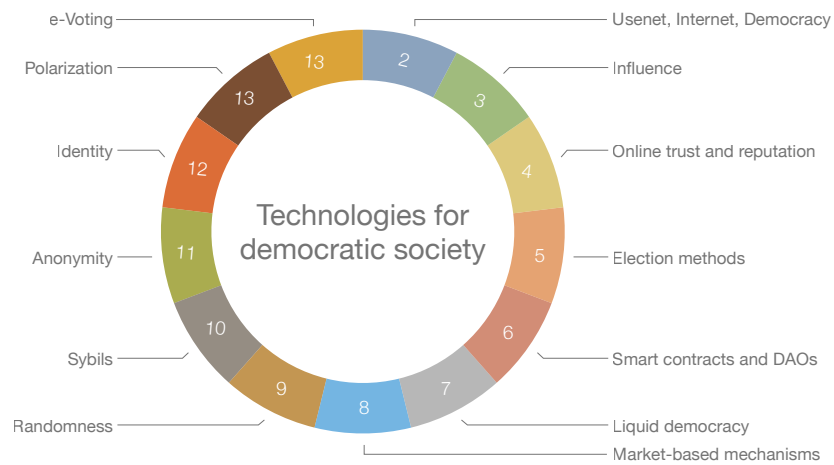
Quiz time - We start at 11:30

## Technologies for democratic society (CS-234)

---

Recap of the semester

Vero Estrada-Galiñanes  
FALL 2023  
EPFL



## Usenet, Internet, democracy (week 2)

---

- A computer as a communication device - Licklider and Taylor
- Individual advantages / Societal advantages
- Problems/risks in communication: exclusivity, filibustering, security & privacy
- Netizens: Usenet - UUCP - BBS | Content organization - Problems
- Robert Dahl's four criterion: Effective participation, voting equality, enlightened understanding, control of the agenda
- A fifth criterion: Inclusivity
- Politics of distraction

## Usenet, Internet, democracy (week 2)

---

State two potential social benefits that UseNet was widely perceived to provide while it was popular, and two social disadvantages or weaknesses it exhibited in the way people were ultimately found to use it.

## Influence (week 3)

---

- How does influence happens
- What measures influence in X (Twitter)? Metrics - Message propagation
- Page Rank algorithm: how does it work? Hint: Linear Optimization Problem
- Academic paper influence
- Money influence - Piketti and Wealth inequality
- Lorenz curve - Gini coefficient

## Online trust and reputation (week 4)

---

- Search engine manipulation. Methods / techniques
- Scientific peer review: Why is relevant?
  - Metrics: impact factor, h-index, ...

## Election methods (week 5)

---

- Why are the possible reasons for gathering collective "will"?
- How preferences can be expressed? Yes/no (approval voting), 1-out-of-n, k-out-of-n, rank set, scoring | See week 7
- How are votes counted or aggregated?
- What are the properties needed for running an election? Transparency, anonymity/privacy, fair, inclusive
- Single-winner election methods. Majority wins. Runoff election. Condorcet Winner & Condorcet Cycle
- Multi-winner: Single transferable vote (STV) | Party-list proportional representation (PR)

## Smart contracts and DAOs (week 6)

---

- Cryptocurrencies 101
  - How is a UTXO transaction validated?
- Tokens: platform tokens, NFT, governance
- What is governance?
- How is a DAO created? How does it work?
- What can go wrong in a DAO? Hint: "The DAO" hack
- Smart contracts. The vending machine analogy. Turing complete languages. Gas limit. Applications
  - Multi-sig contracts

## Liquid democracy (week 7)

---

- Direct democracy vs Representative democracy
- Proxy voting
- Liquid democracy
  - Google pilot
- Voting methods - Tally methods

## Market-based mechanisms (week 8)

---

- Fundraising models
- Crowdfunding
- Dangers of democratizing fundraising
- Prediction markets. How do they work? Applications. What can go wrong?
- Quadratic voting? How does it work? Problems
- Vote pricing rule

## Randomness (week 9)

---

- Deciding the right candidate: Three main risks
- Benefits of randomness
- Applications of randomness in democratic processes: Tie breaking - Athens - Venice - Census - Opinion polling
- Terms: Sortition - Kleroteria
- The Republic of Venice. The Doge selection
- Deliberative polling | Citizen assemblies

## INTERLUDE

### Students feedback via Moodle

---

- Log onto moodle and stay on the moodle home page (dashboard).
- Click on the arrow to the top right of the screen which will reveal a block that contains the entitled “In-depth evaluation” title (please note: all evaluations will be together in the evaluation tile on the moodle home page, and not separate in each course moodle page).
- Students can then select your course and complete the feedback.
- Students will also be able to access the course evaluations via the EPFL Campus App.

### Sybils (week 10)

---

- Online identity
- Why do we want to limit the number of accounts?
- Defense mechanisms: cost-based and human-centric
- Identity in p2p networks
- Human-centric mechanisms: KYC, reputation-based, PGP, Kleros, HumanityDAO
- Trust network approaches to detect Sybil's
- Biometry: INDIA cases / Worldcoin
- Proof of personhood / Pseudonymous party

### Anonymity (week 11)

---

- Reasons for anonymity: Privacy. Freedom
- Anonymity for context / purpose
- “Dark side” - Vote stuffing
- Balance: Anonymity vs Identity. Accountability
- Other mitigations.

### Identity (week 12)

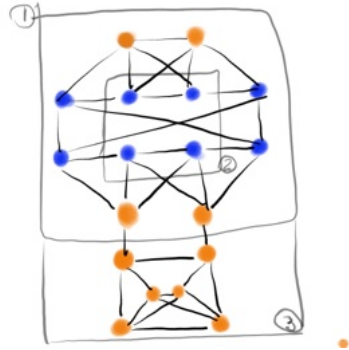
---

- Characteristics of identifiers
- Zooko's triangle: Security. Human-Readable. Decentralized
- Type of identifiers: Random number. Registration authority. Blockchain
- Name Mapping. Examples: x.509. PGP. Blockchain
- Namecoin's “squatting” problem. ENS solution
- Decentralized identity
- Verifiable claims. How do they work? Where do we store credentials
- Other properties for identity: Sybil-resistance - Privacy-preserving - Self-sovereign

## Polarization (week 13)

---

- Radicalization. Metrics used by the scientific study. Limitations of the study
- Information gerrymandering
- Group social dilemma:
  - compromise worldview
  - zero-sum worldview



## e-Voting (week 13)

---

- Why using technology for voting?
- What are the risks?
- Hybrid e-voting | Remote voting | Online voting
- Components: machine - printer - ballots - ballot box
- End-to-end verifiability: Cast as intended - Recorded as intended - Counted as recorded
- Technological solutions: Blockchain, cryptographic primitives, verifiable receipts
- Problems of verifiable receipts