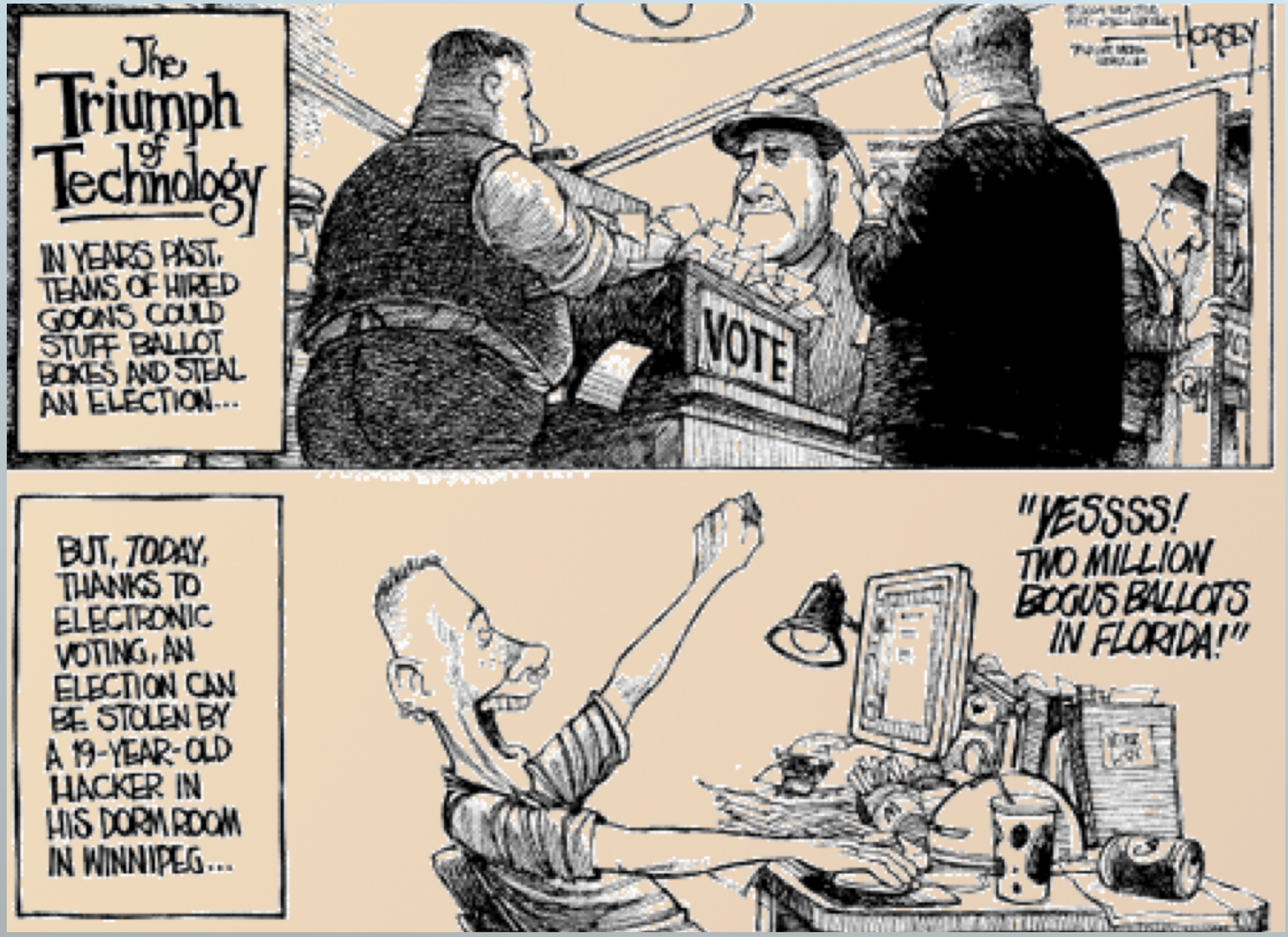
E-voting : A simple problem (TP)



TO DO : Open a web browser (firefox?)
You should go to my home page and click on the link:
"Semaine Transverse : the problem with e-voting"

Home Page for J. Paul Gibson (B.Sc, Ph.D, HDR)

Département - INFormatic

Location: Bureau D311, Le département INFormatic, Telecom SudParis (TSP), 9 rue Charles Fourier, 91011 Évry cedex, FRANCE

Research: L'Unité Mixte de Recherche SAMOVAR (Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux) UMR 5157 INT CNRS Research Laboratory, Equipe METHODES (Méthodes et modèles pour les réseaux),

jpaulgibson, @JPaulGibson
email: paul.gibson@telecom-sudparis.eu, Phone/Fax: +33(0)1-6076 (4477/4711), Contact/Annuaire TSP

A recent CV is available in English or French (français).

My Web Pages

- Research
  - Publications and Invited Presentations
  - Conferences/Workshops: committees and reviewing
  - Supervision: PhD, MSc and BSc.
  - Evaluation/Reviewer: journals, projects and theses.
- Current Teaching (2015/16)
  - Undergraduate TSP -
    Semaine Transverse - The problem(s) with e-voting
    CSC3101 - Algorithmique et langage de programmation
    CSC3502 - Projet Informatique
    CSC4102 - Introduction au génie logiciel pour applications orientées objet
    CSC4504 - Langages formels et applications
    CSC4522 - Projet système d'information : réalisation et déploiement
    CSC5524 - Industrialisation d'un projet système d'information: software quality, metrics, tests, process improvement
  - Postgraduate TSP -
    MSc Computer & Communication Networks (CCN):
    CSC7003 - Foundations of Software Engineering
    CSC7203 - Object Oriented Computing and Distributed Systems
    CSC7336 - Software Engineering For Smart Devices
  - Formation Continue (Further Education) - Steria Architect Academy
- Personal Pages

External Links

IMPEX ANR research project

CS Unplugged

Annals of telecommunications (Springer Journal)

ISoLA 7TH INTERNATIONAL SYMPOSIUM ON LEVERAGING APPLICATIONS OF FORMAL METHODS, VERIFICATION AND VALIDATION

SHONAN MEETING Implicit and Explicit Semantics Integration In Proof Based Developments Of Discrete Systems.

Special Issue Journal
- The role of telecommunications in E-voting

http://www-public.tem-tsp.eu/~gibson/Teaching/SemaineTransverse/E-voting-problems/

E-voting : A simple problem (TP)

Teaching-SemaineTransverse/E-voting-problems for Dr J. Paul Gibson, INFormatique (INF), Telecom SudParis, France.

Semaine Transverse - E-voting Problems

In this short TP we will be looking at some of the problems that are associated with e-voting machines. You will be presented with some on-line voting machines and you will have to experiment with them to see if they function as required.

Scratch Machines On-Line: machine 1, machine 2, machine 3, machine 4

The machines are written using Scratch, a simple graphical programming language for teaching beginners to programming (often, but not always, young children)

Lecture Slides

E-voting Problems slides,

Additional reading material

A Review of E-voting: the past, present and future, J Paul Gibson, Robert Krimmer, Vanessa Teague and Julia Polmares. Published in Springer Annals of Telecommunications, volume=71, number=7, pages=279--286, July 2016
PDF Springer Link d 10.1007/s12243-016-0525-8

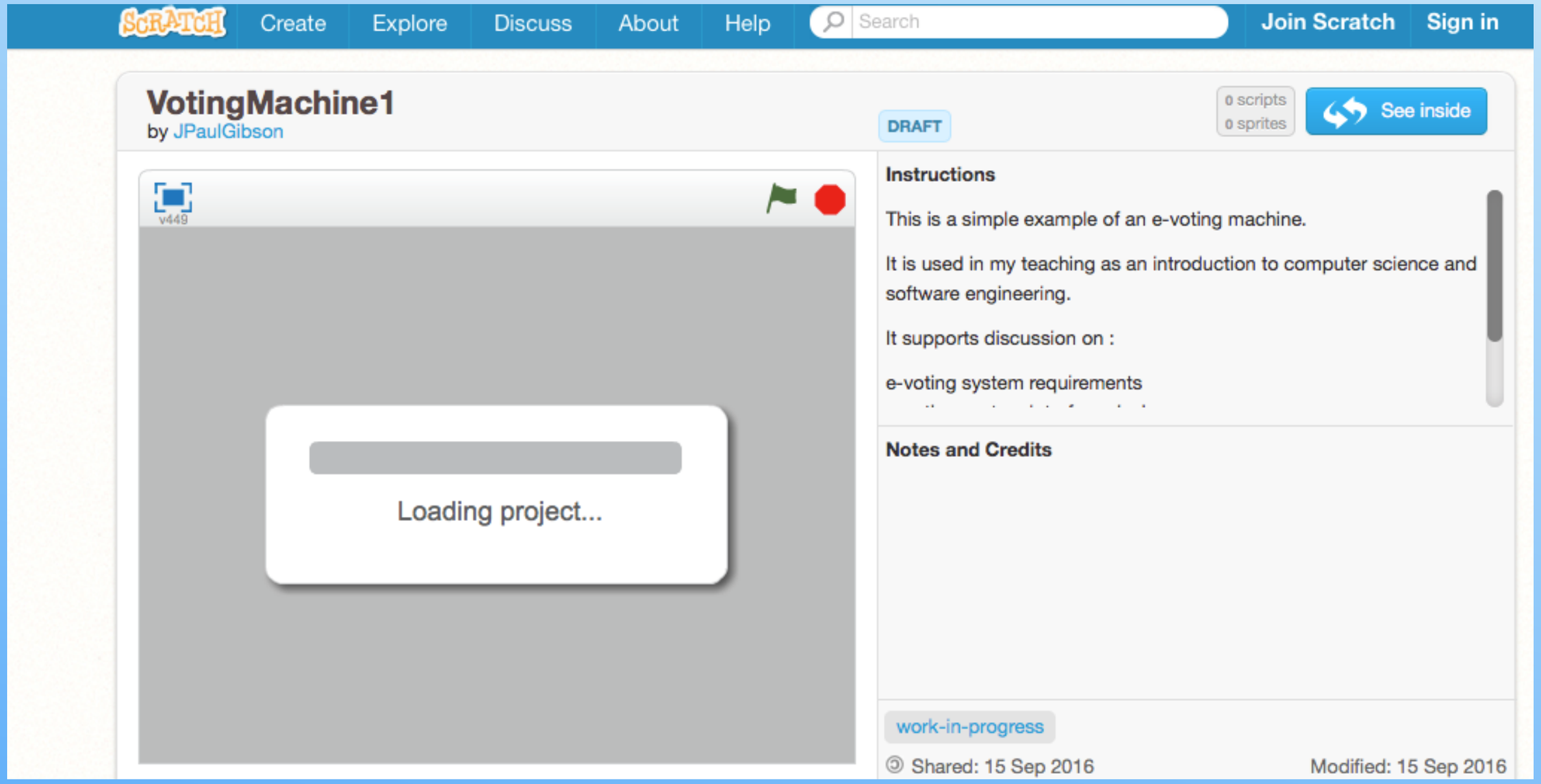
Useful Links

Scratch Programming

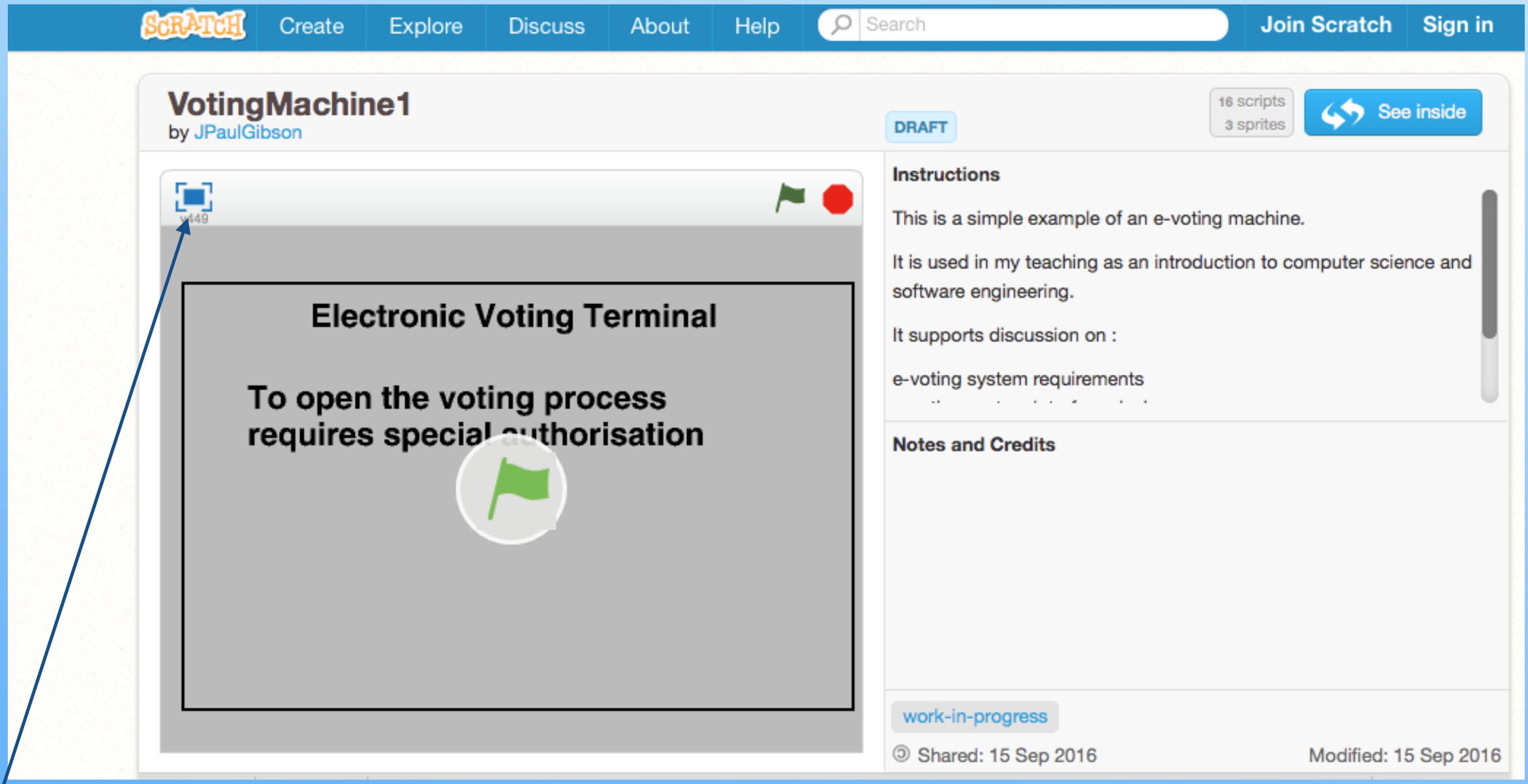
URL: http://www-public.telecom-sudparis.eu/~gibson/Teaching/SemaineTransverse/E-voting-problems/ Last Revision: 15th September 2016 Contact: paul.gibson@telecom-sudparis.eu

TO DO : click on the first Scratch machine1

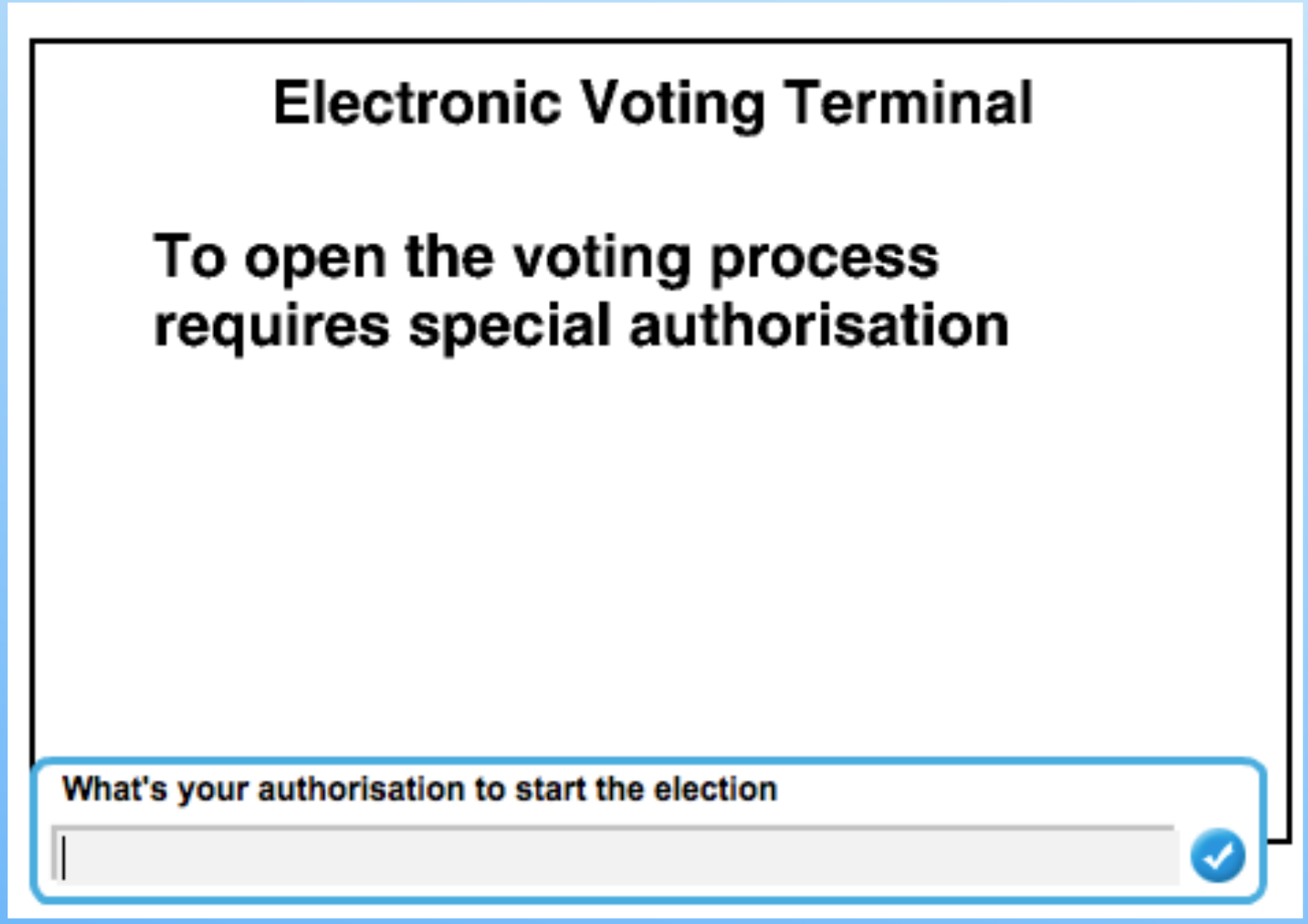
TO DO: wait until the project has loaded



TO DO: run the machine by pressing on the green flag



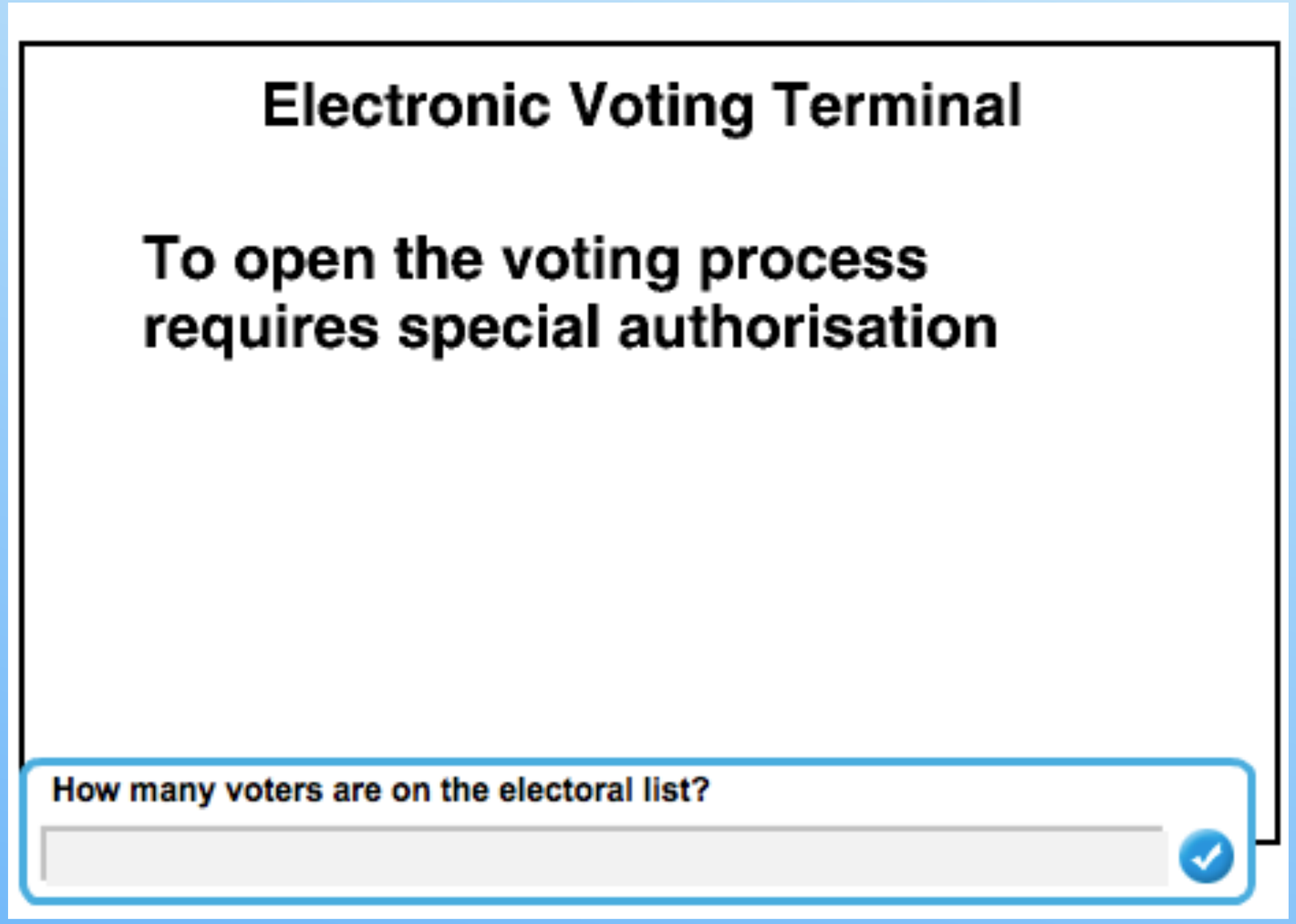
You can go to full screen mode



Can you guess the authorisation password?

It is surprising how many e-voting systems are not secure

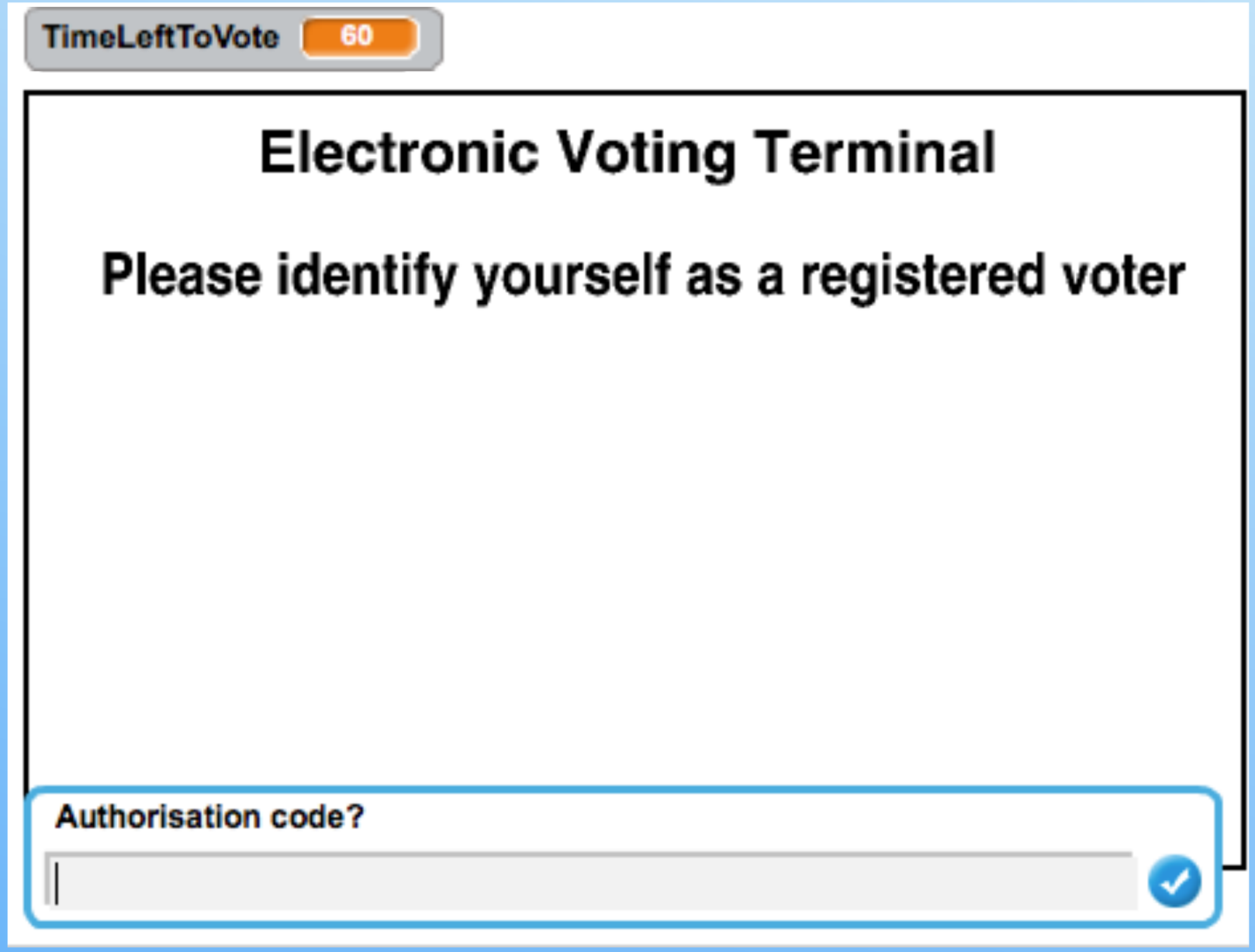
E-voting : A simple problem (TP)



Election configuration is usually more complex, but even in this simple case the administrators can make mistakes

TO DO : Test which values are considered valid

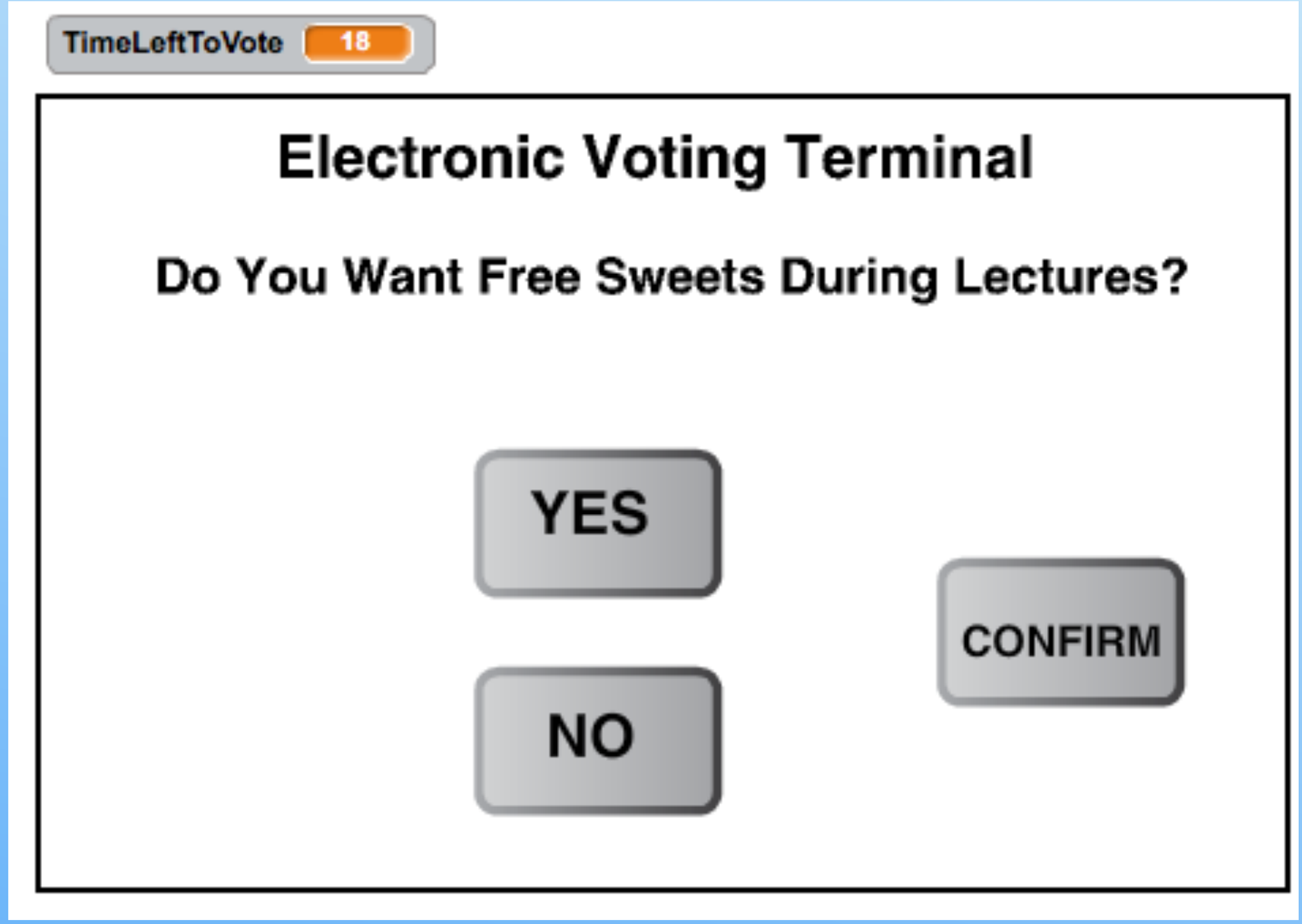
E-voting : A simple problem (TP)



Voter authentification is usually complex, but here each voter has a unique ID number between 0 and n-1

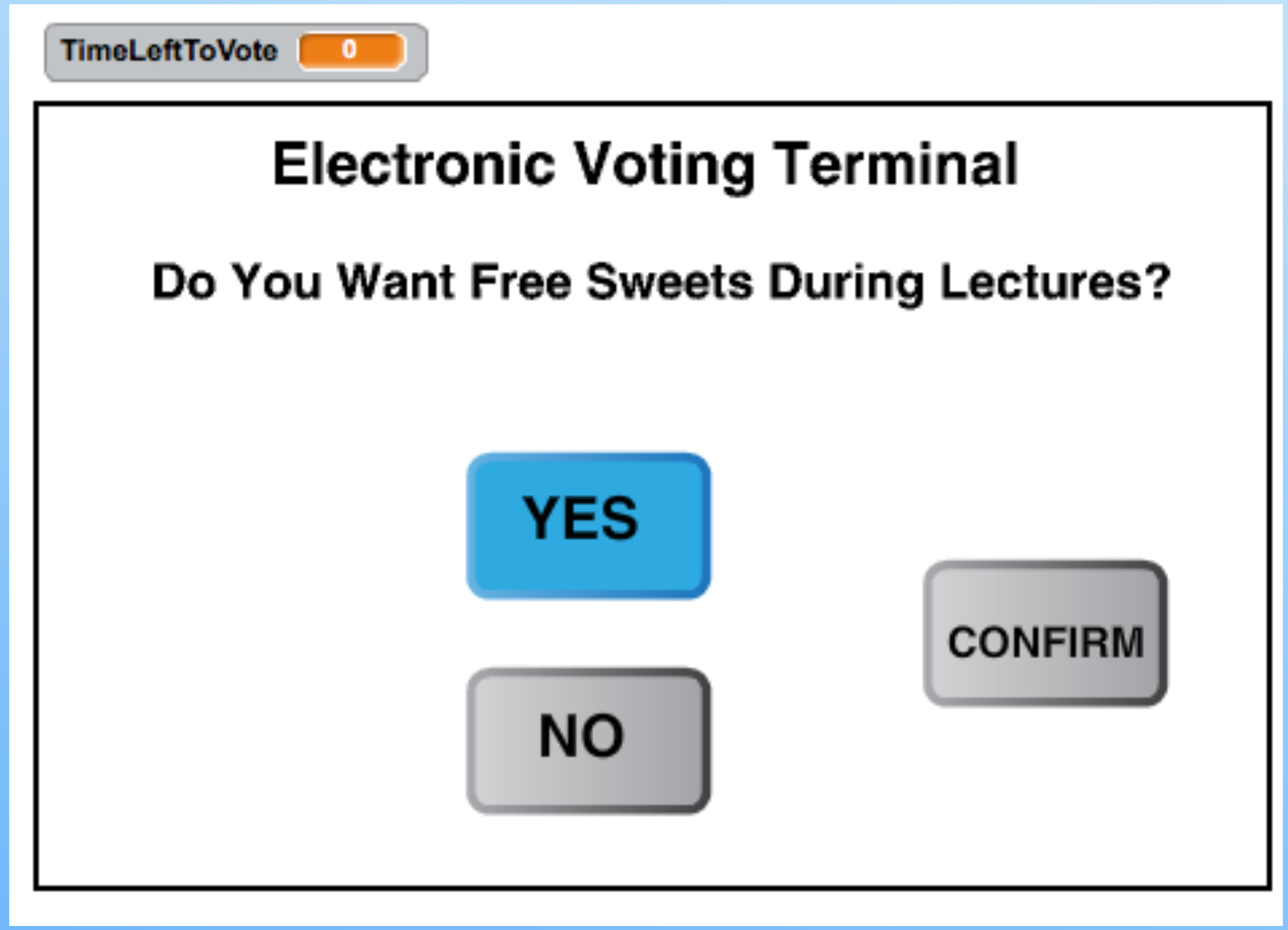
Question : is this sort of code a good idea?

E-voting : A simple problem (TP)

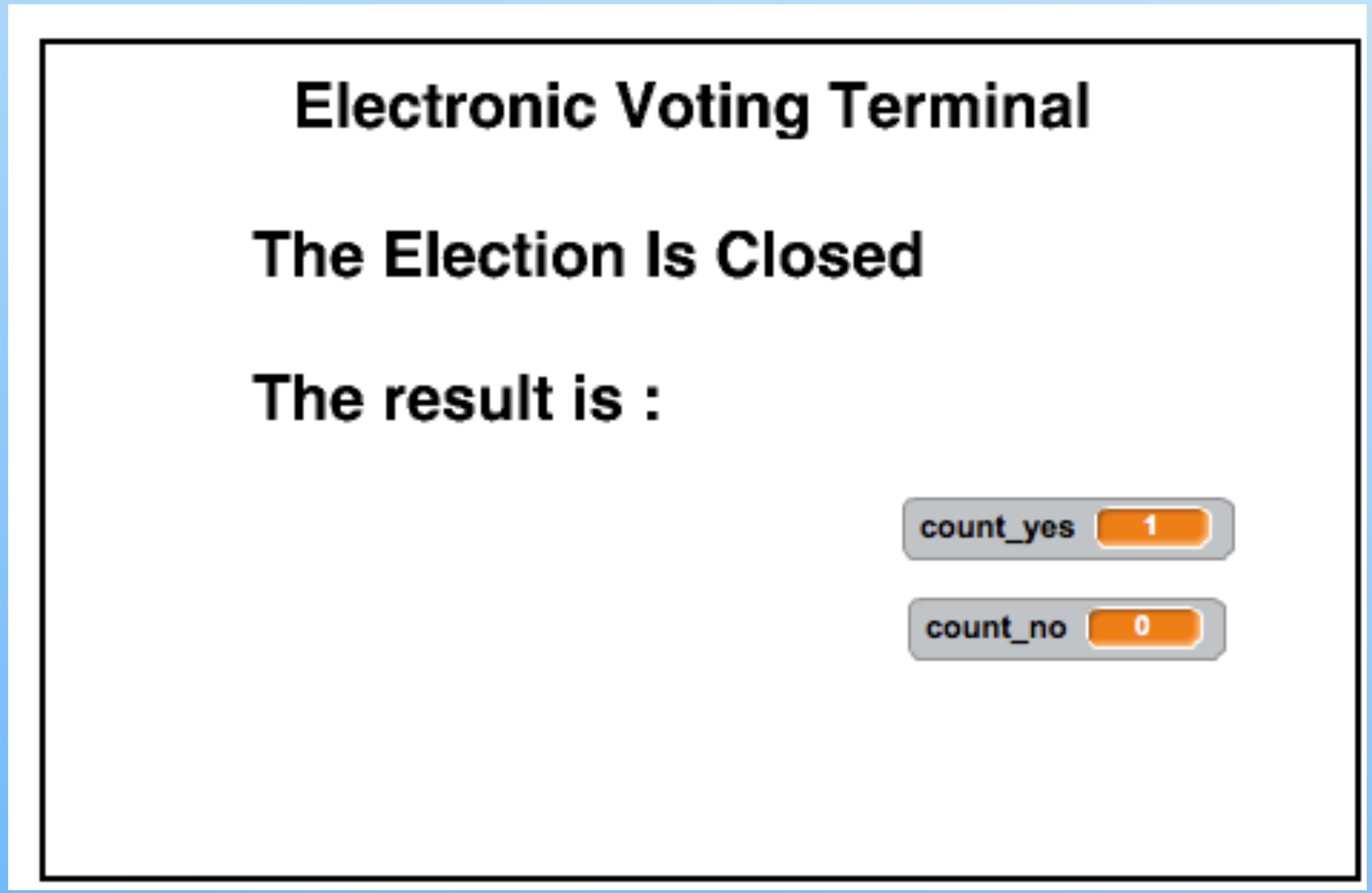


TO DO : Test if the interface works *correctly*

E-voting : A simple problem (TP)



QUESTION : what happens if the time runs out in the middle of voting?

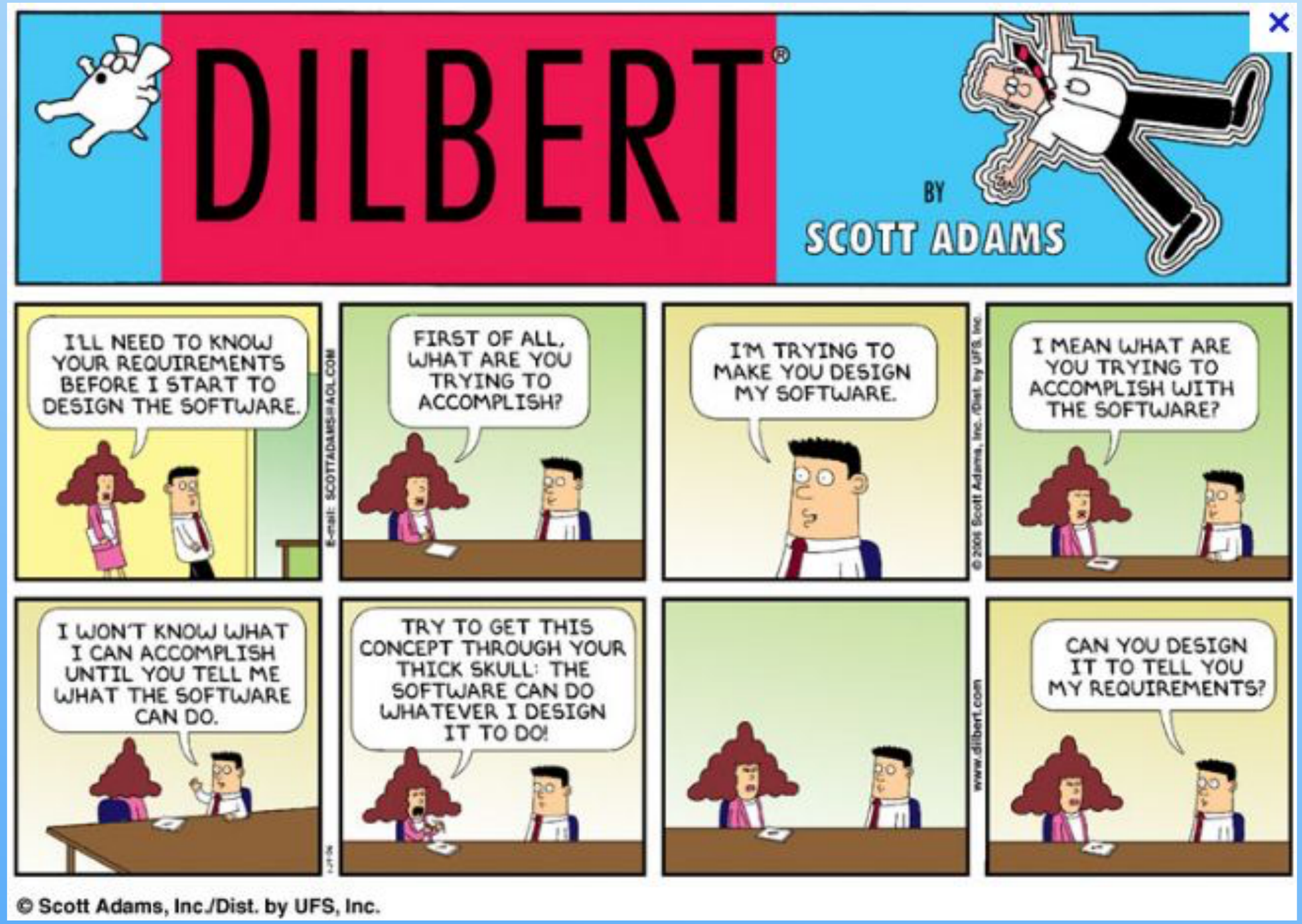


Does the election count the votes *correctly*?

Is the machine *acceptable*?

E-voting system requirements

What requirements do you think a voting system should meet?



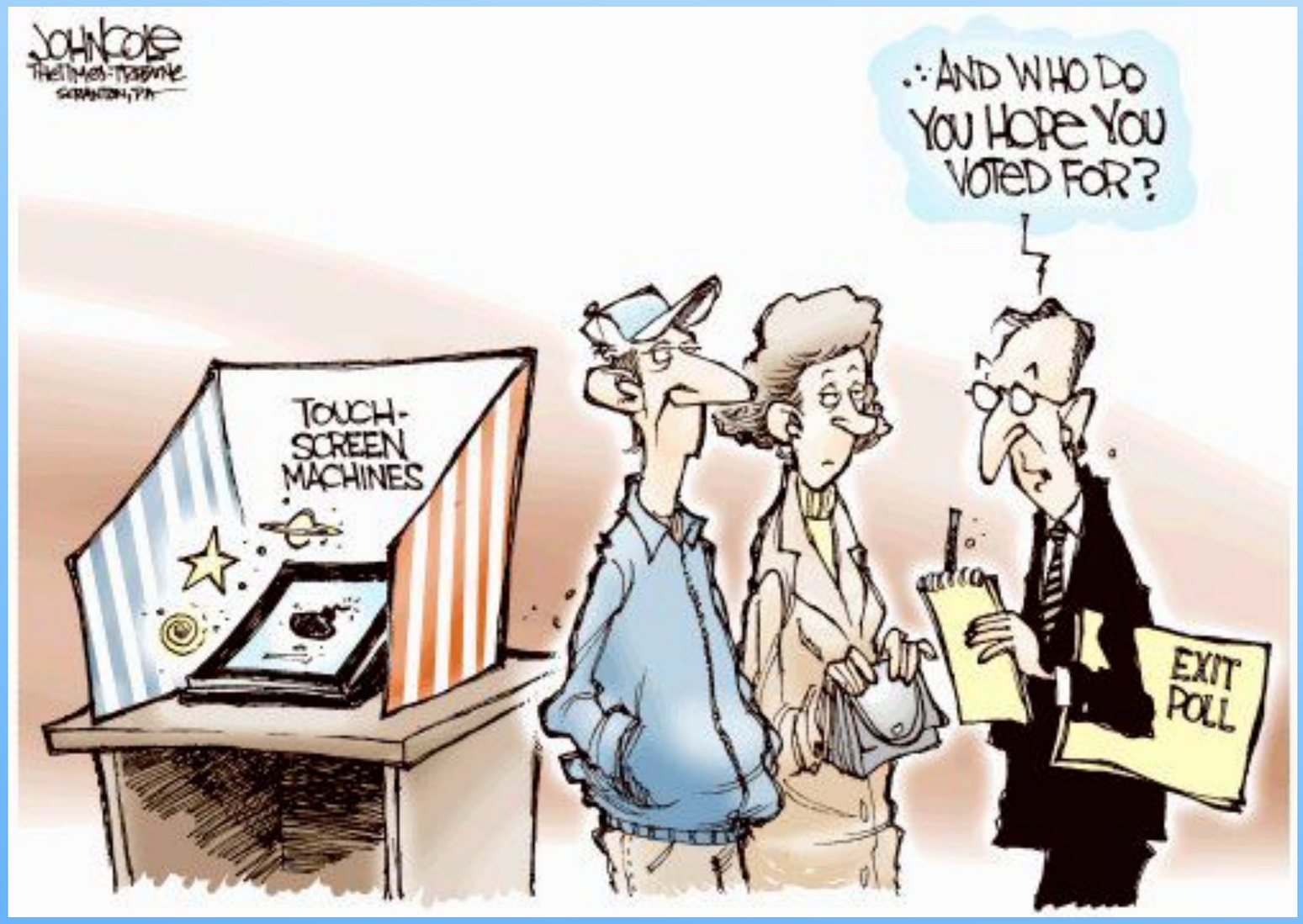
E-voting system requirements

What requirements do you think a voting system should meet?

TRUSTWORTHY - TRUSTED???

E-voting system requirements

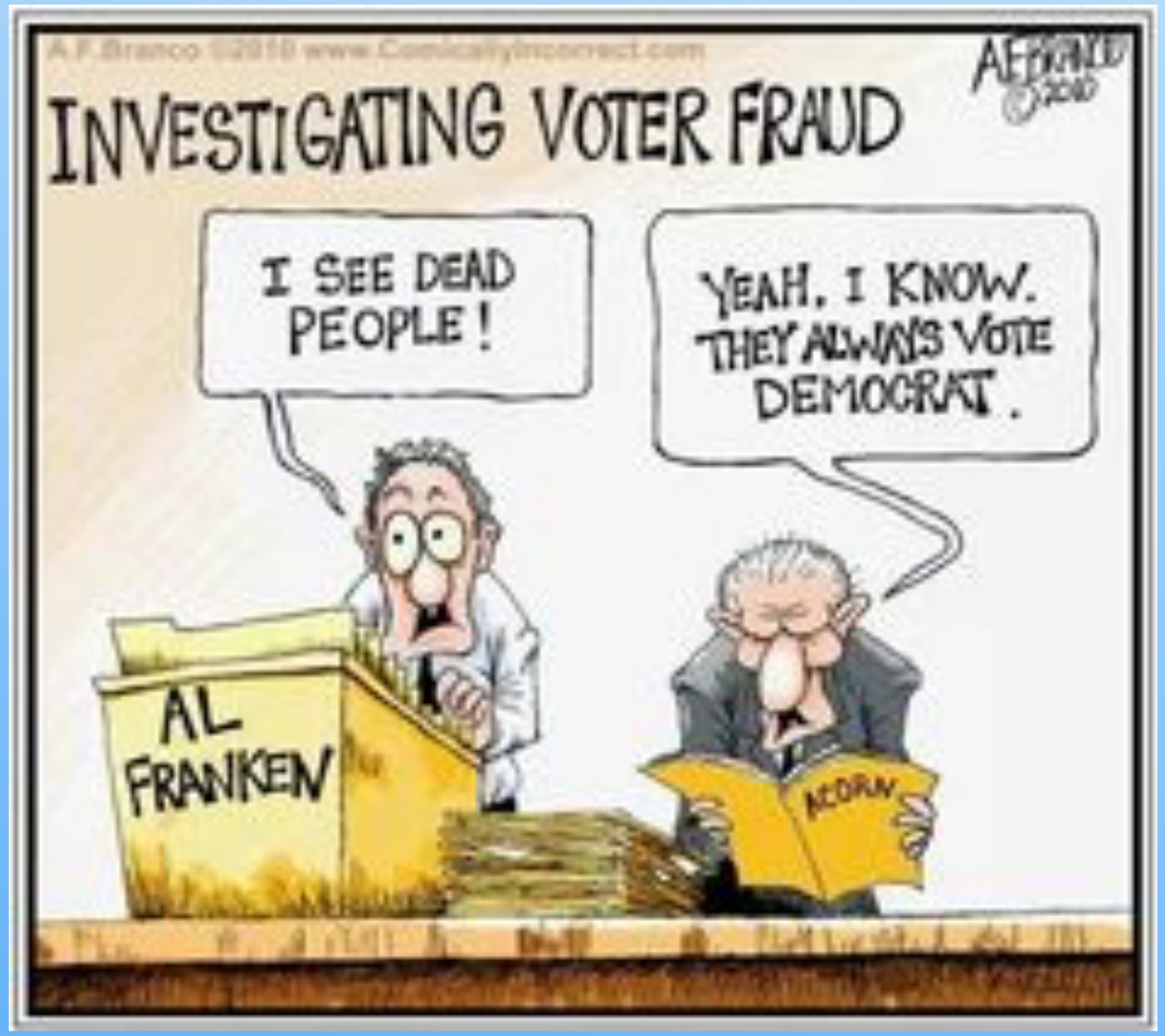
What requirements do you think a voting system should meet?



RELIABLE - DEPENDABLE???

E-voting system requirements

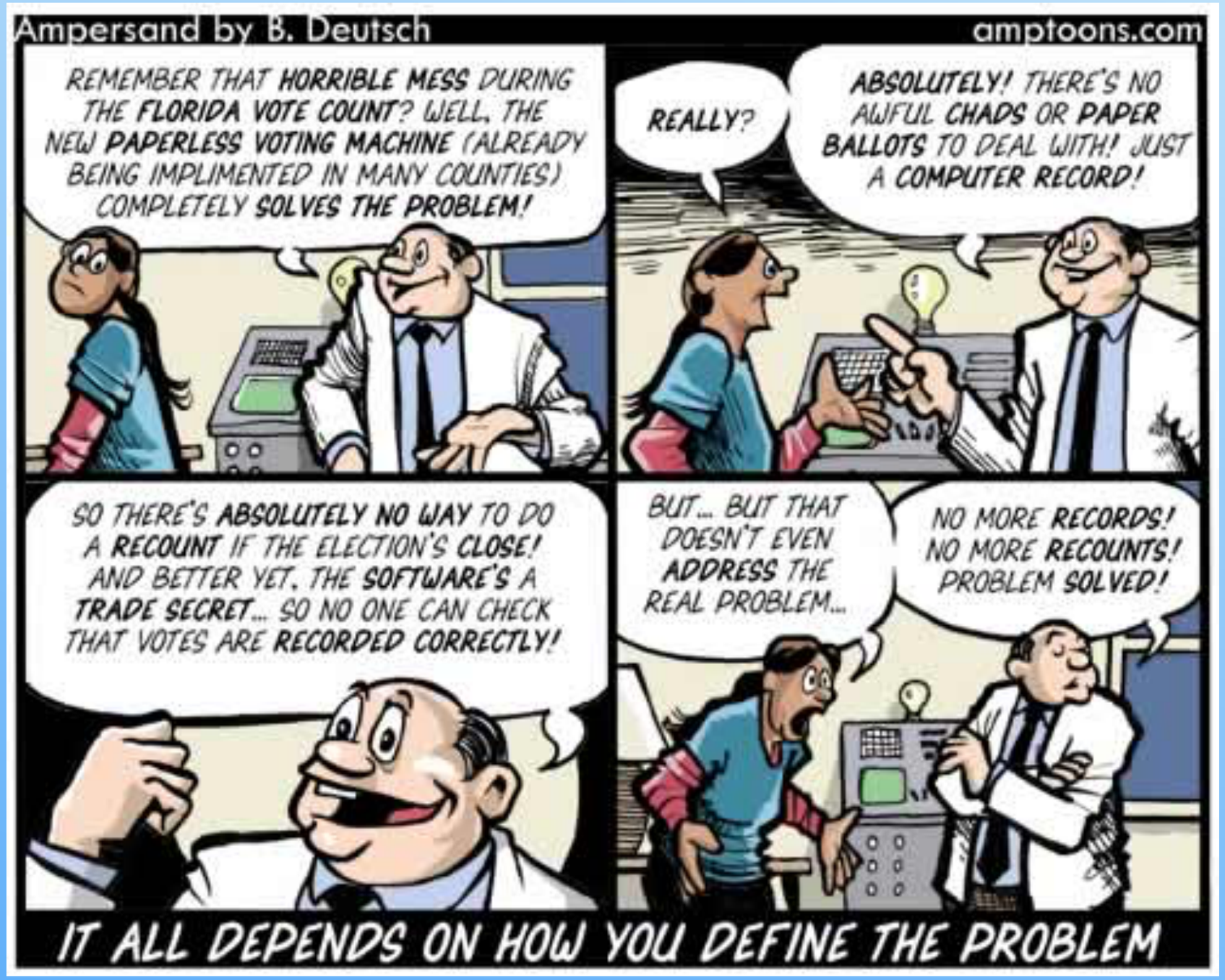
What requirements do you think a voting system should meet?



SAFE AGAINST FRAUD???

E-voting system requirements

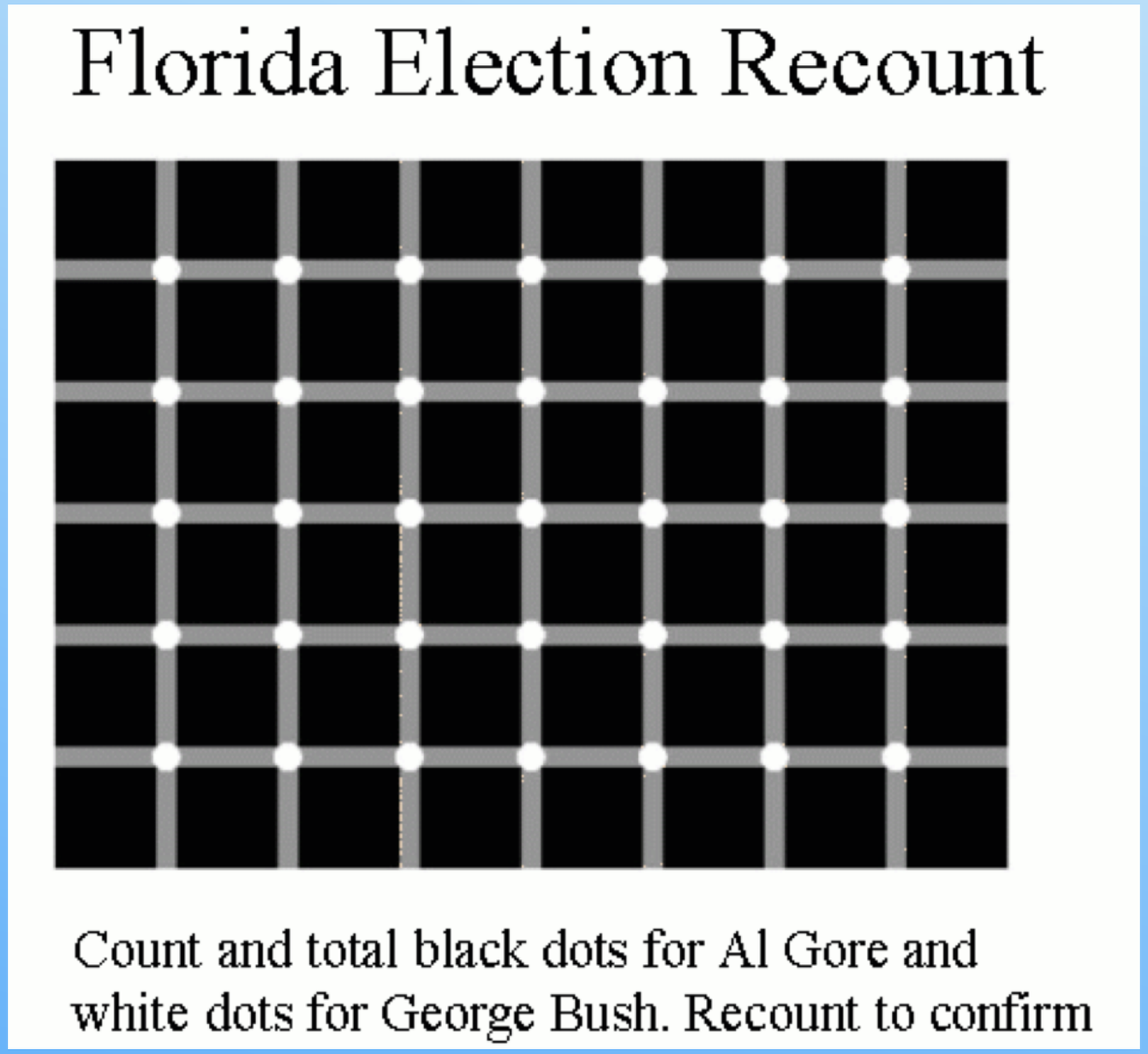
What requirements do you think a voting system should meet?



AUDITED??

E-voting system requirements

What requirements do you think a voting system should meet?



RECOUNTABLE ??

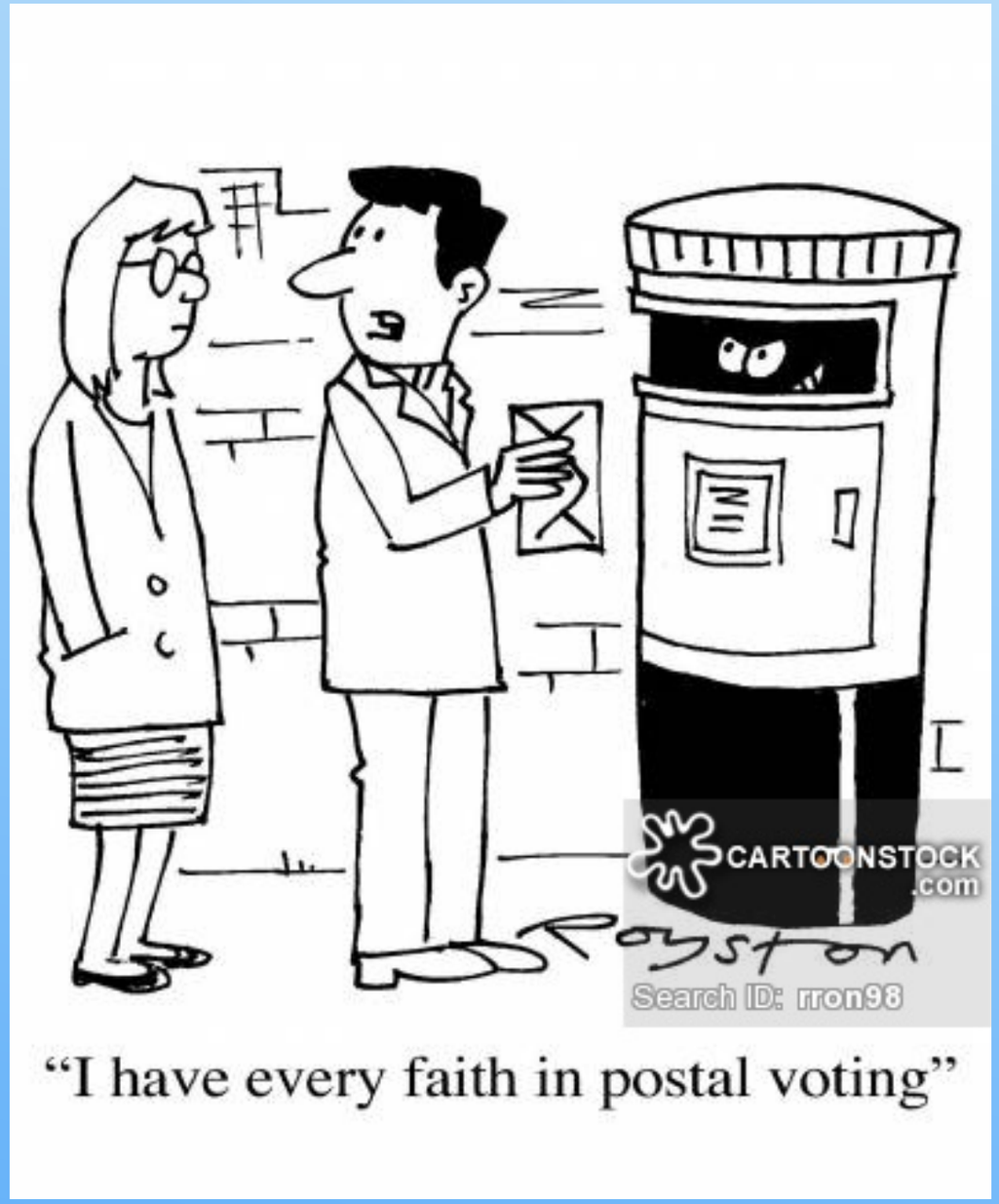
E-voting system requirements

What requirements do you think a voting system should meet?

RECEIPT-FREE ??

E-voting system requirements

What requirements do you think a voting system should meet?

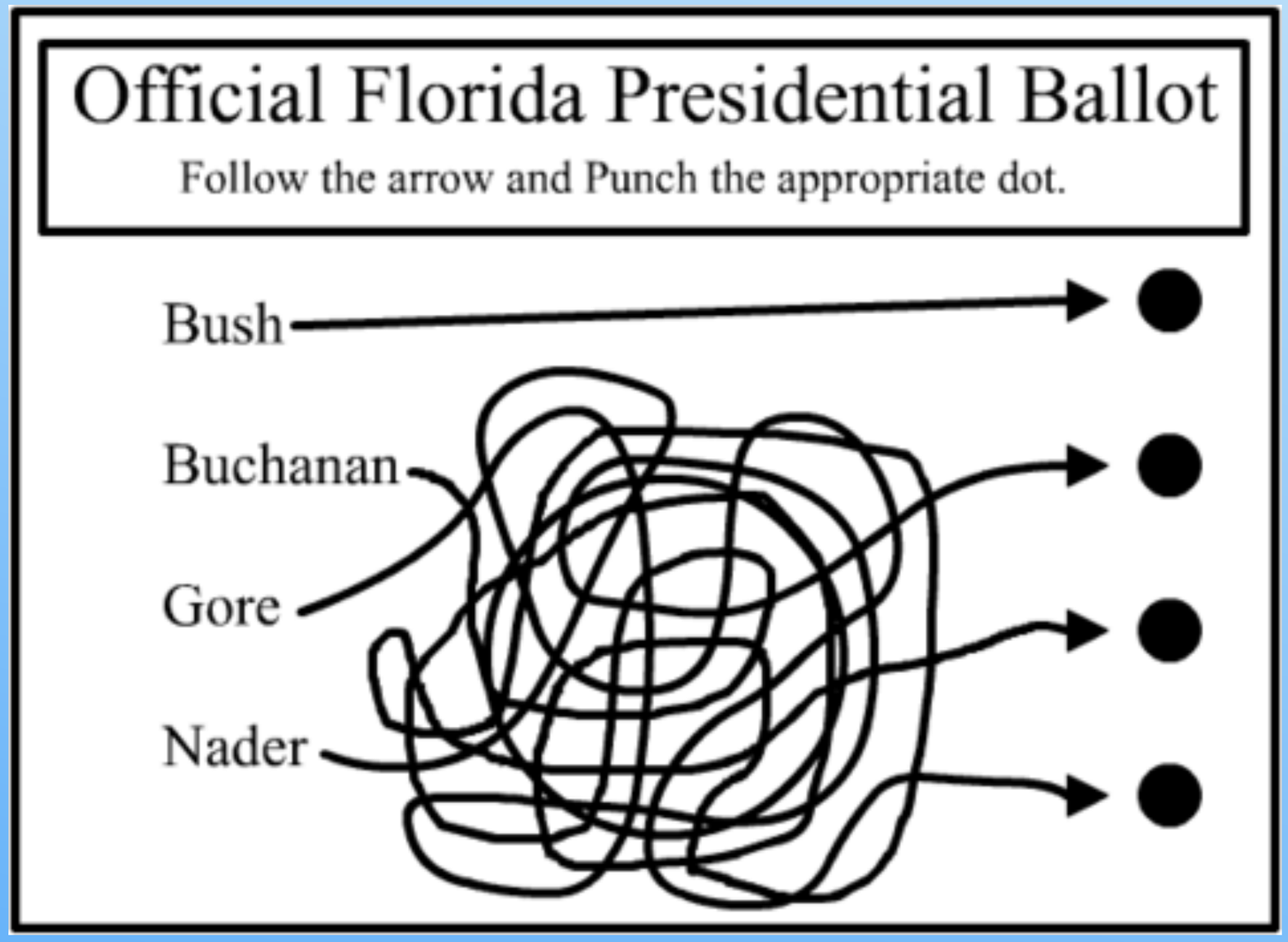


"I have every faith in postal voting"

ON A NETWORK??

E-voting system requirements

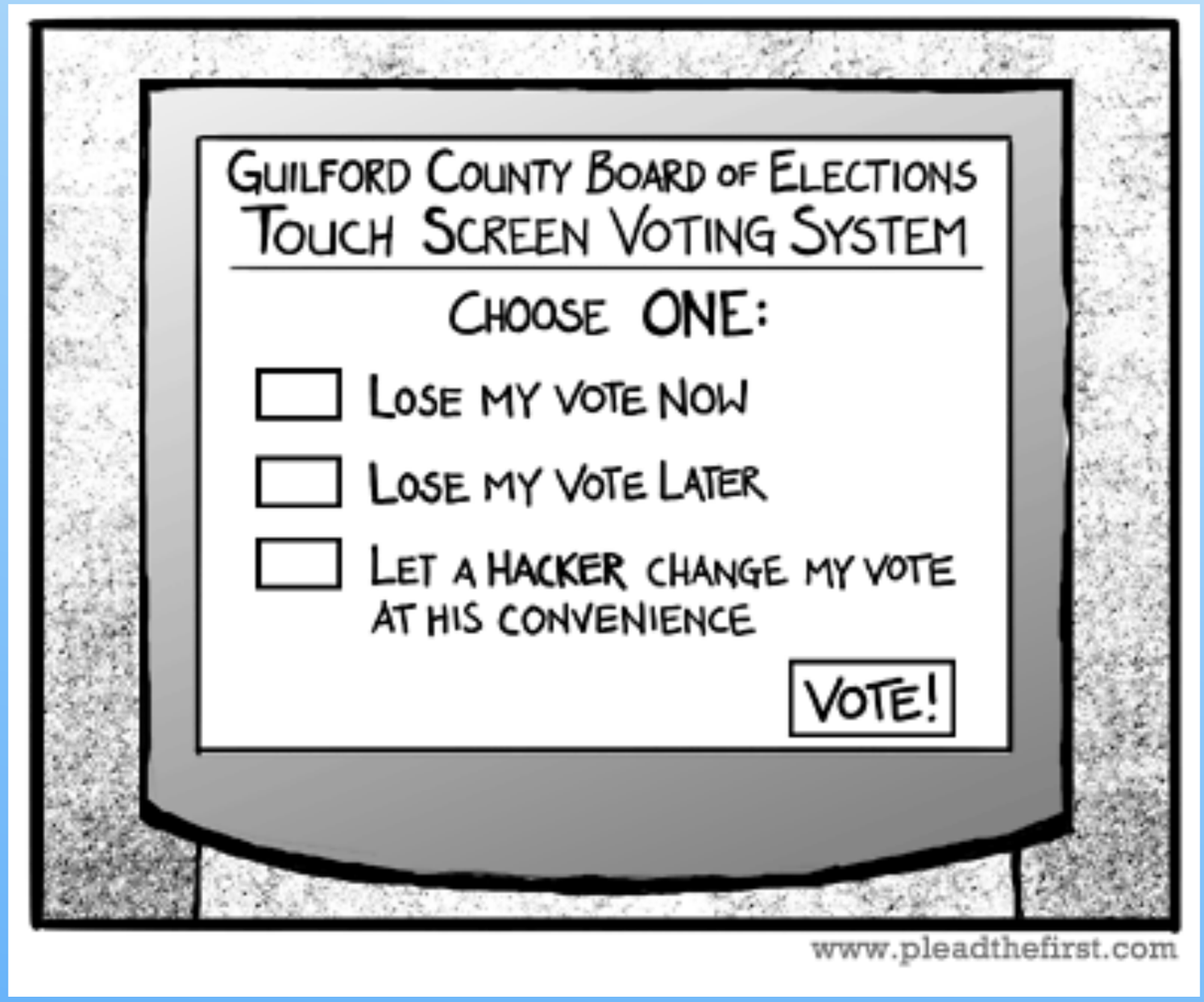
What requirements do you think a voting system should meet?



USABLE??

E-voting system requirements

What requirements do you think a voting system should meet?



SECURE AGAINST ATTACKS

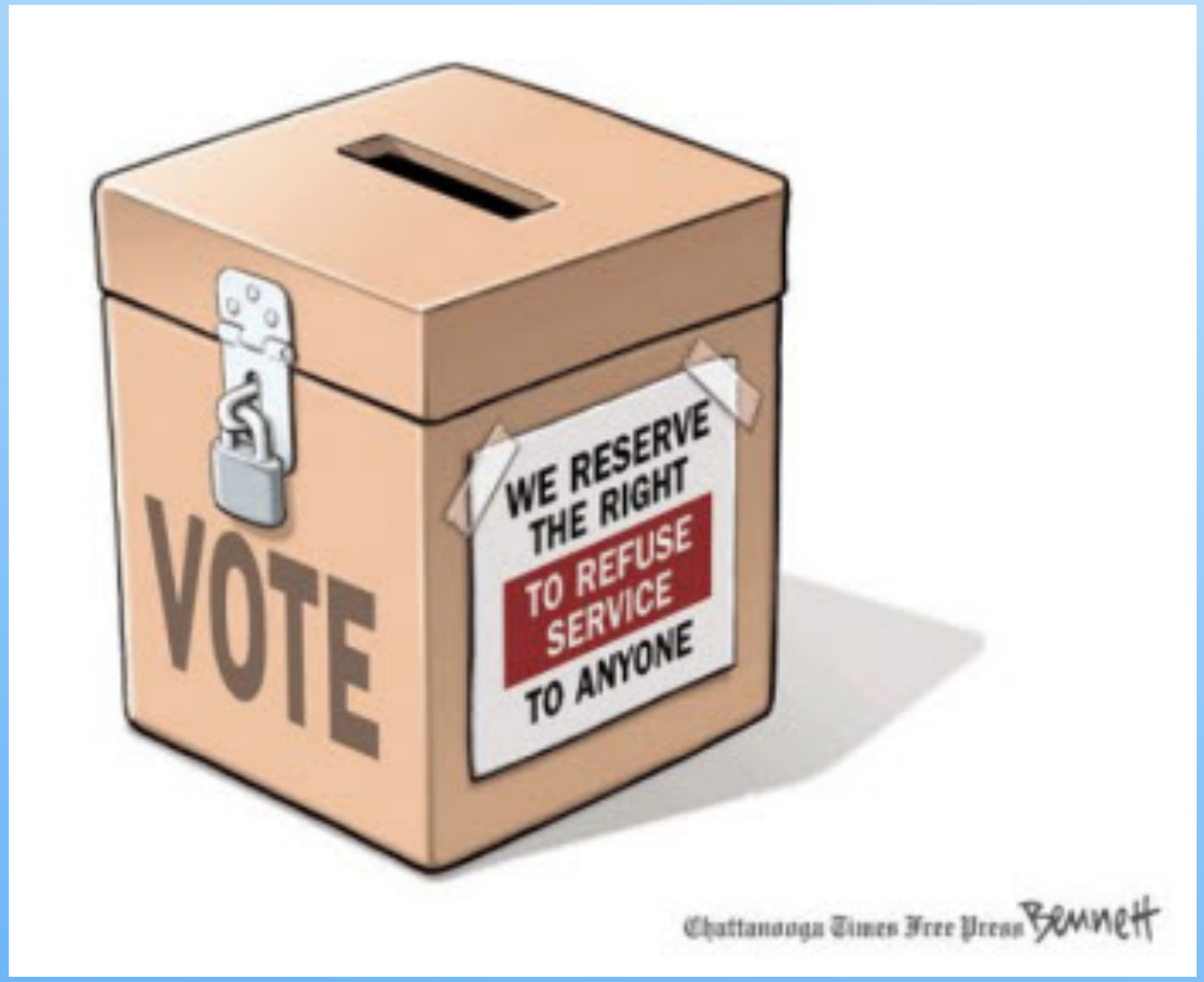
E-voting system requirements

What requirements do you think a voting system should meet?

OPEN / TRANSPARENT ??

E-voting system requirements

What requirements do you think a voting system should meet?



ACCESSIBLE

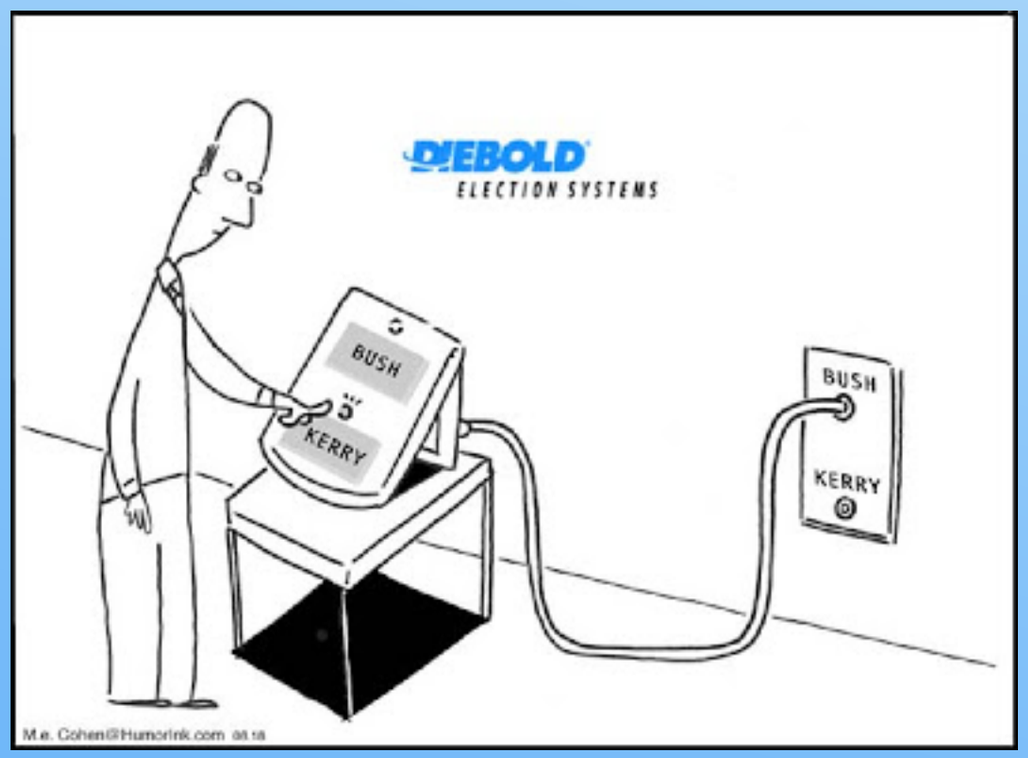
E-voting system requirements

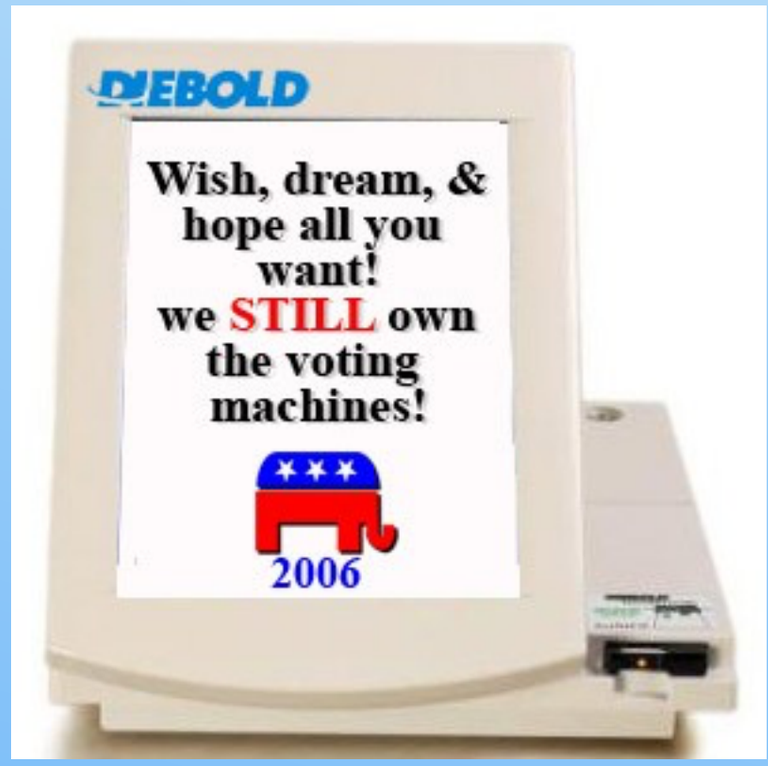
What requirements do you think a voting system should meet?

(FULLY) ELECTRONIQUE?

E-voting system requirements

What requirements do you think a voting system should meet?





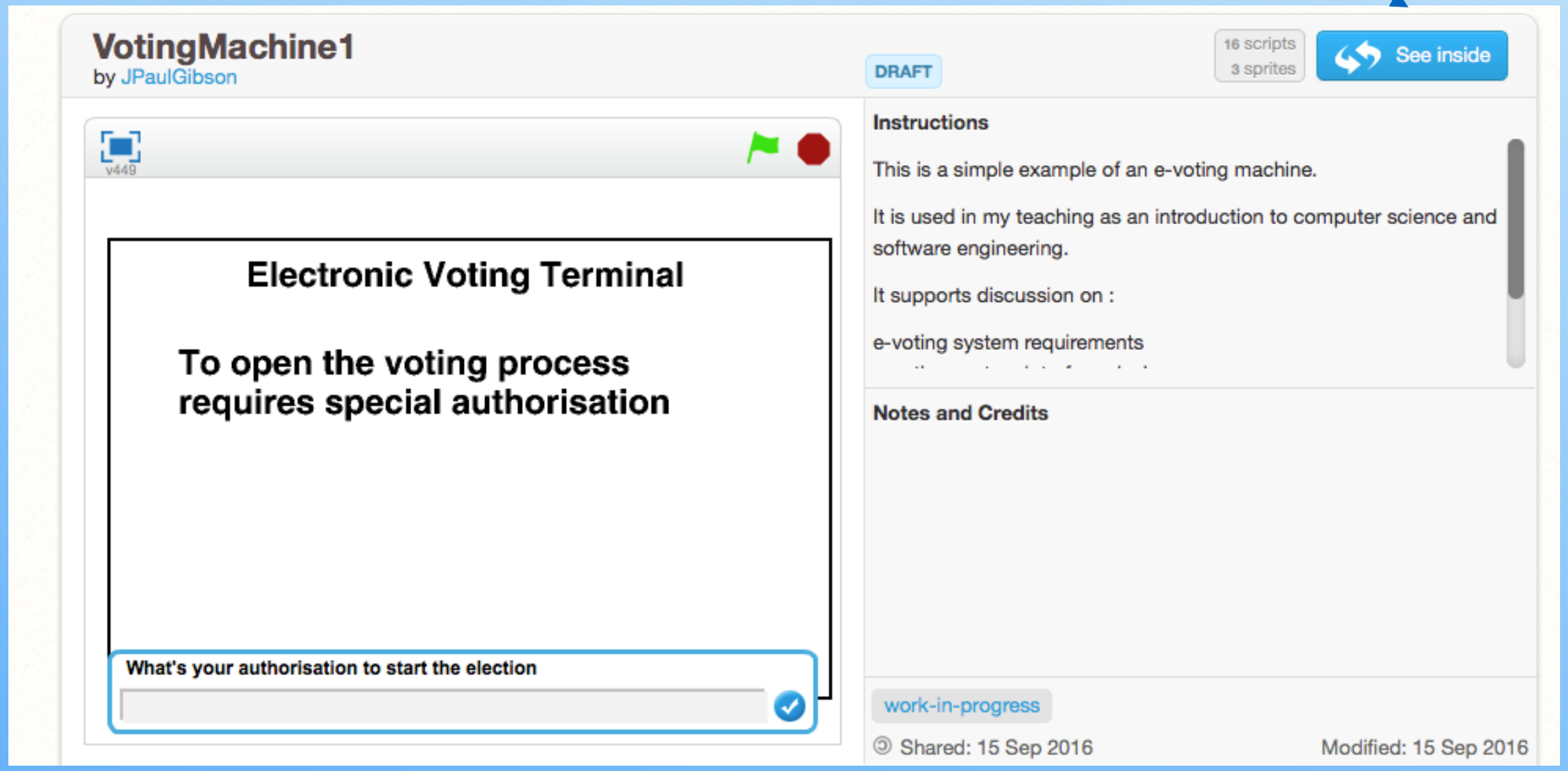
OWNED BY 'YOU'??

E-voting system requirements

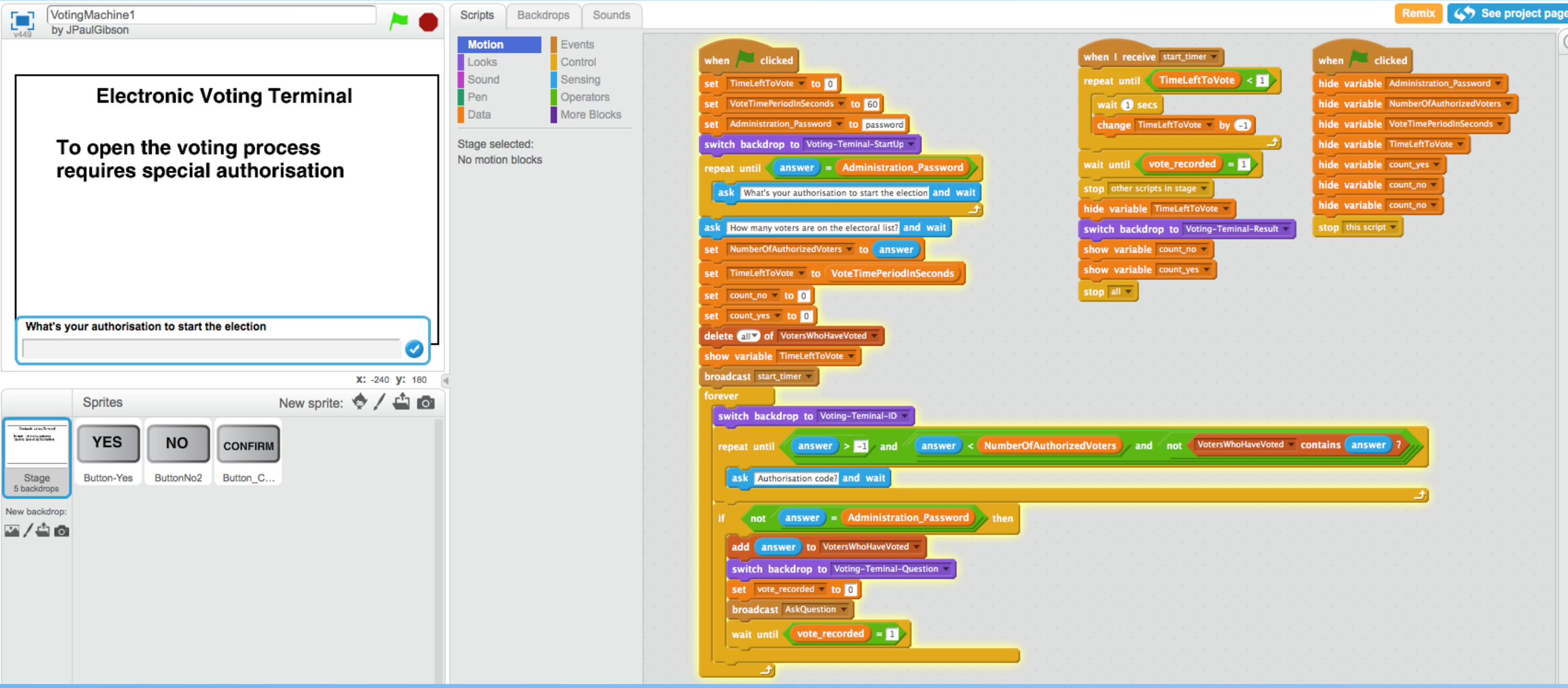
What requirements do you think a voting system should meet?

Coercion-resistant ??

E-voting system - let's look inside at the code



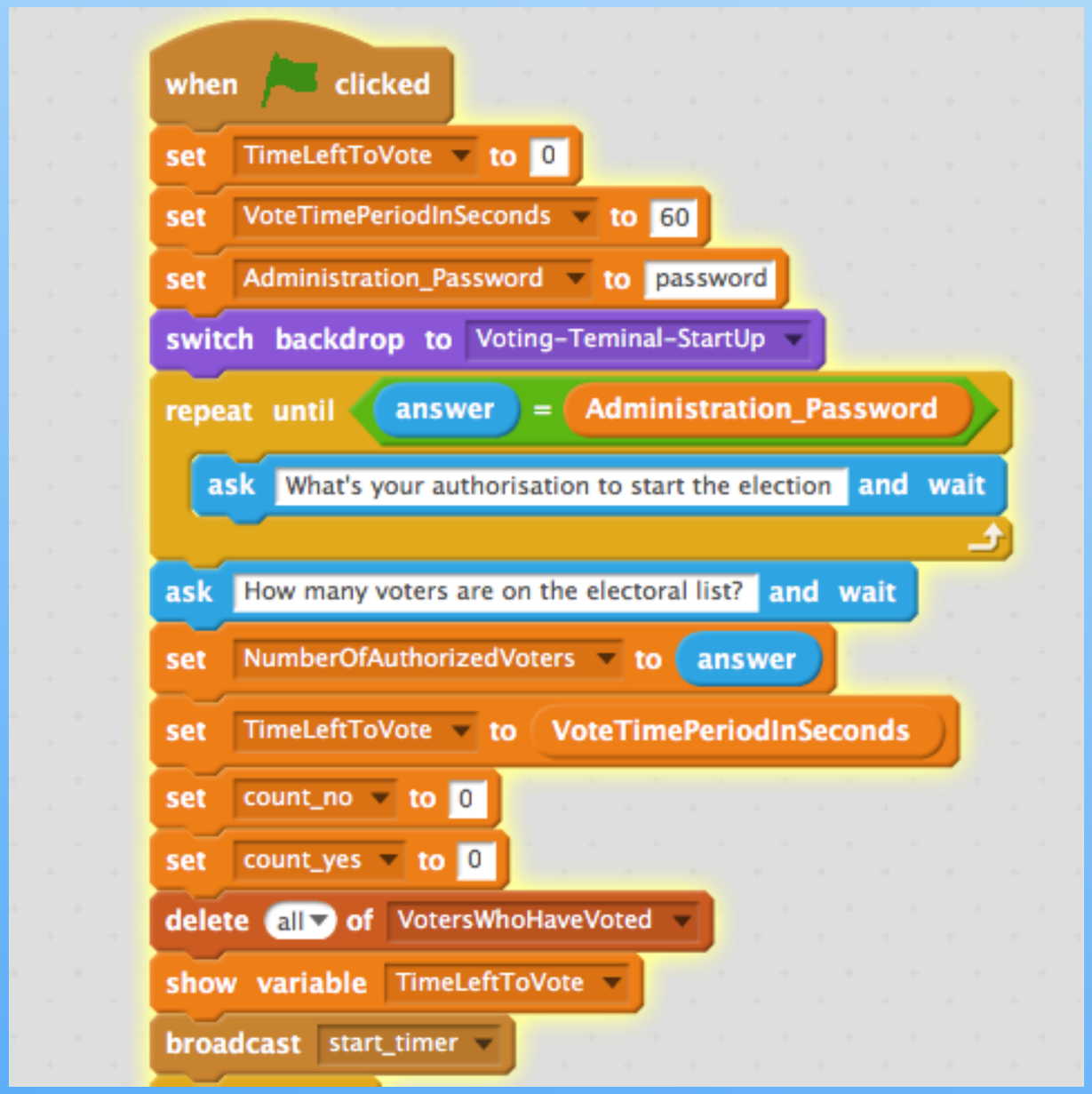
E-voting : A simple problem (TP)



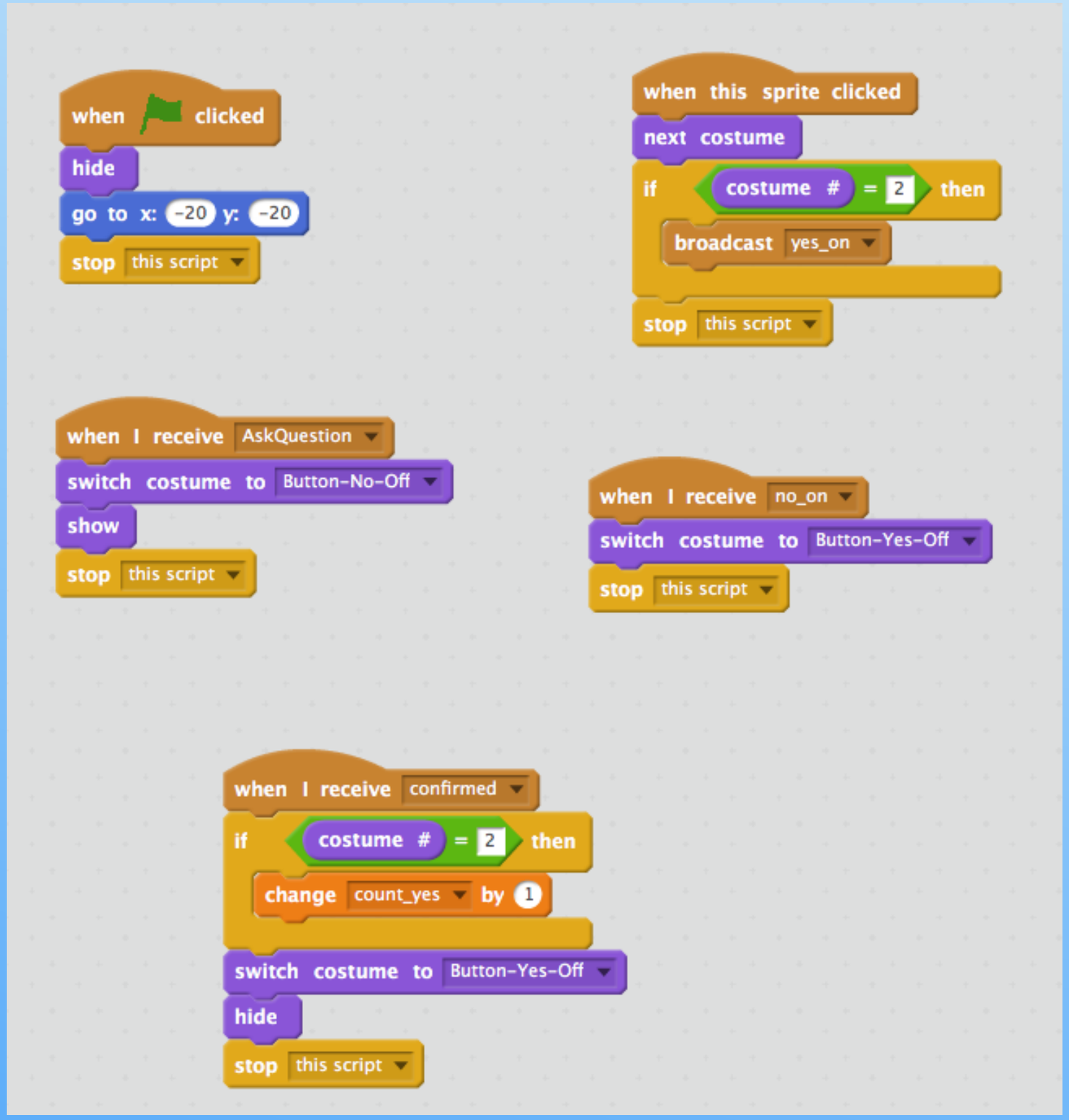
Have any of you ever programmed in Scratch?

Key concepts : backdrop , sprites, scripts

Should e-voting system code be open/visible to the public?

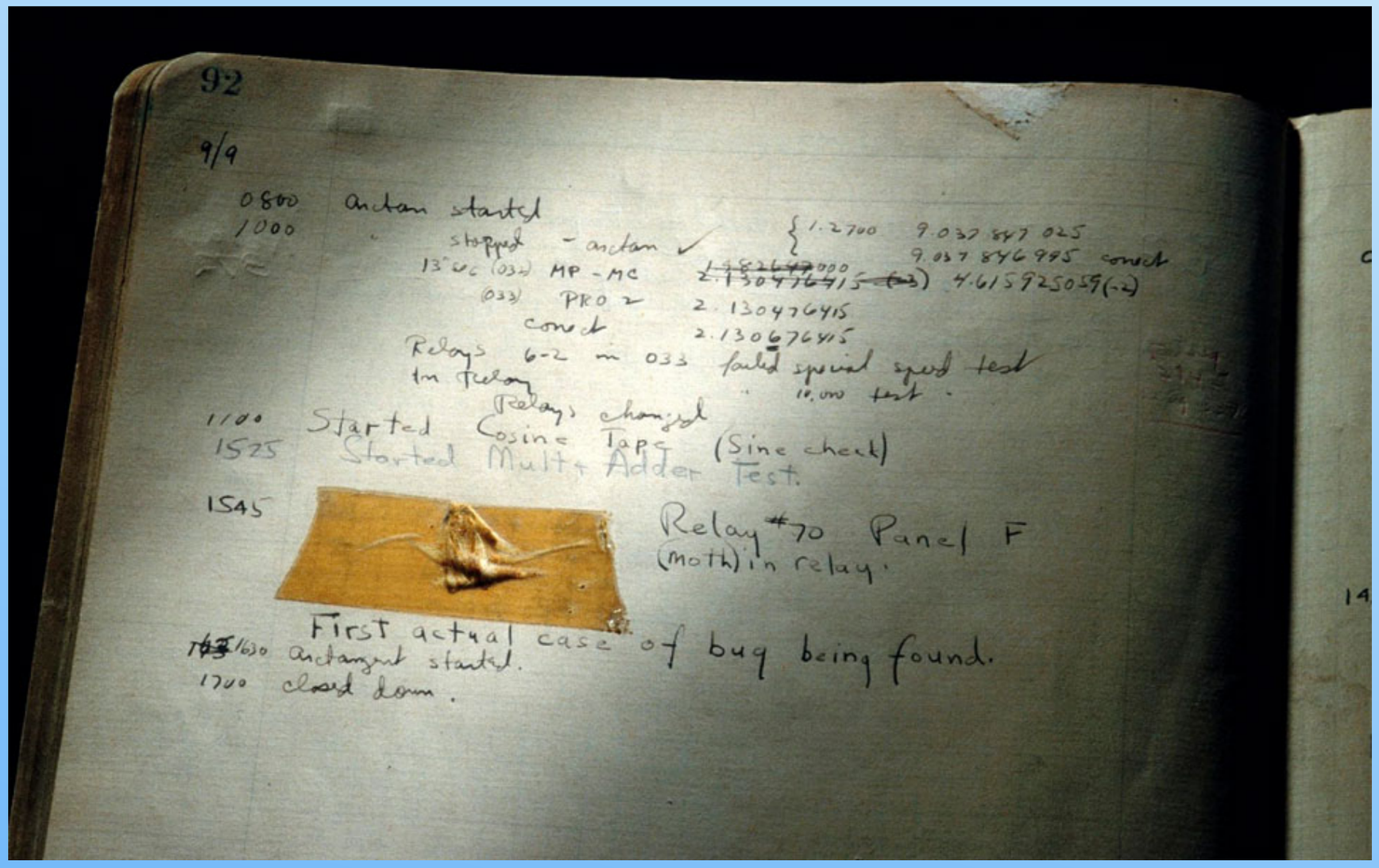


Here is the code for election set-up



TO DO: can you understand the button (YES) code?

Much of the code in e-voting systems has been found to contain ‘bugs’



https://en.wikipedia.org/wiki/**Grace_Hopper**

Much of the code in e-voting systems has been found to contain 'bugs'

When these are found, it may be :

1. ***acceptable*** **human error**
2. **incompetency**
3. **fraud/corruption**

QUESTION: How would you *judge* between these?

QUESTION: Who is responsible for making sure that the e-voting systems are bug-free?

TO DO: Examine the 3 other voting machines, and find the 'bugs' in each of them. They make minor modifications to the first machine that we have tested/analysed. They are based on bugs that have been found in real/deployed voting systems.

QUESTION:

for each machine bug do you judge it most likely to be caused by:

1.*acceptable* human error, or
2.incompetency, or
3.fraud/corruption , or …. ?