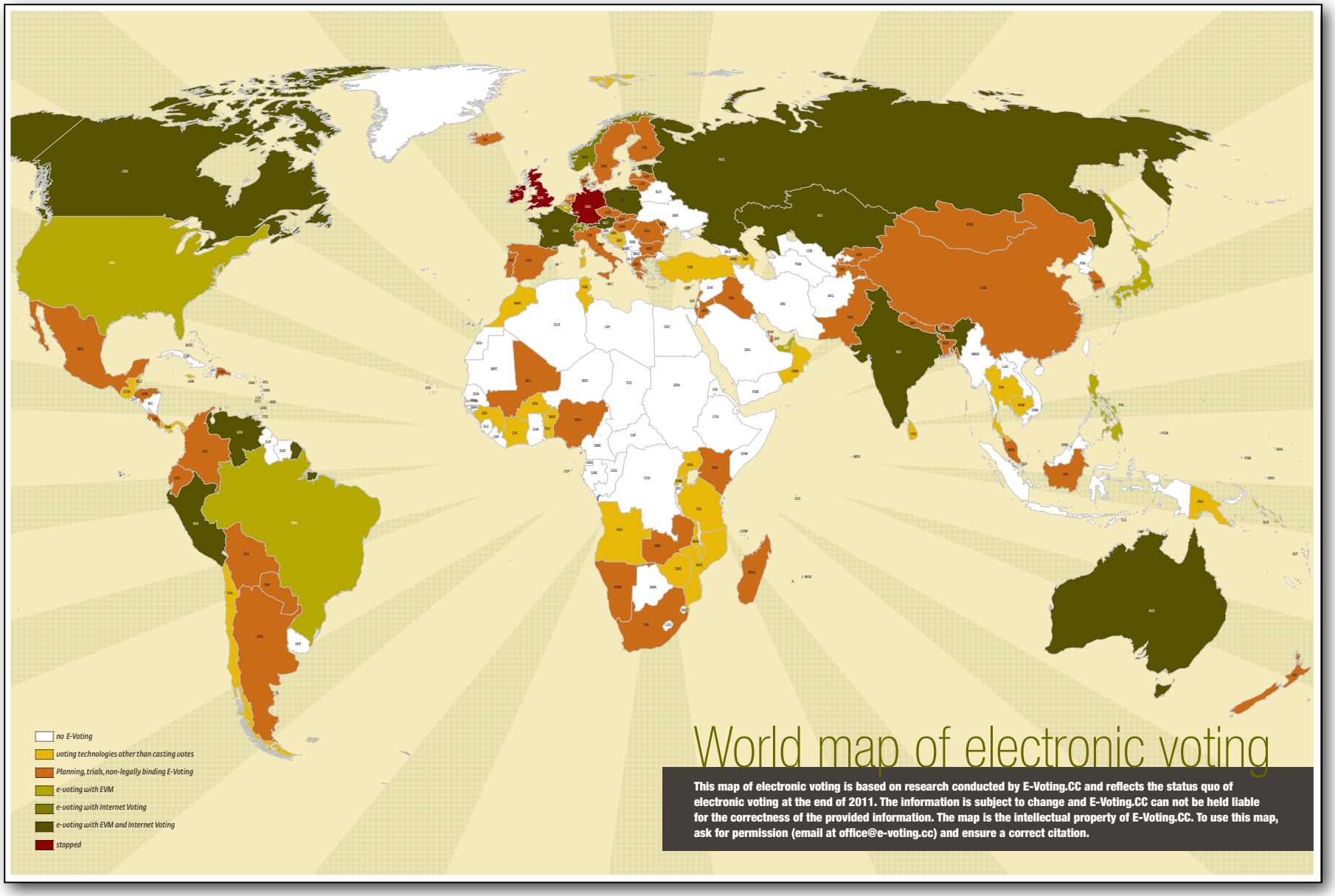
Saving Democracy from Technology

Joseph Kiniry
Technical University of Denmark
1 February 2013

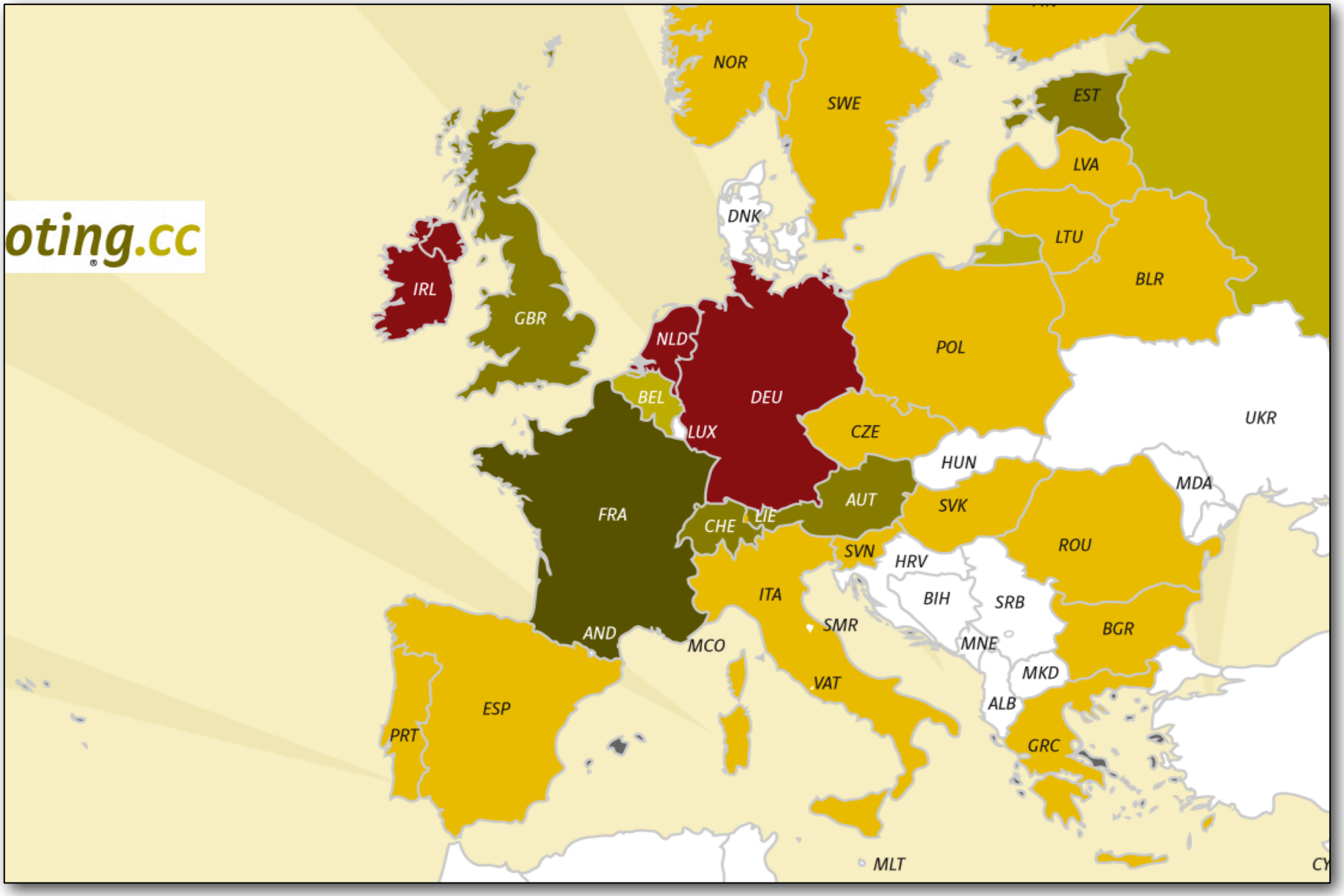
Open Source Elections

- democracy is a critical system
- elections work when they are accurate, secure, and have the trust of the electorate
- elections with digital components must have the same degree of accuracy, security, and maintain the trust of the electorate
- consequently, all digital components (if any) of an election must be accurate, secure, public, non-proprietary, transparent, and comprehensible to all voters

Evoting Worldwide



Evoting in Europe

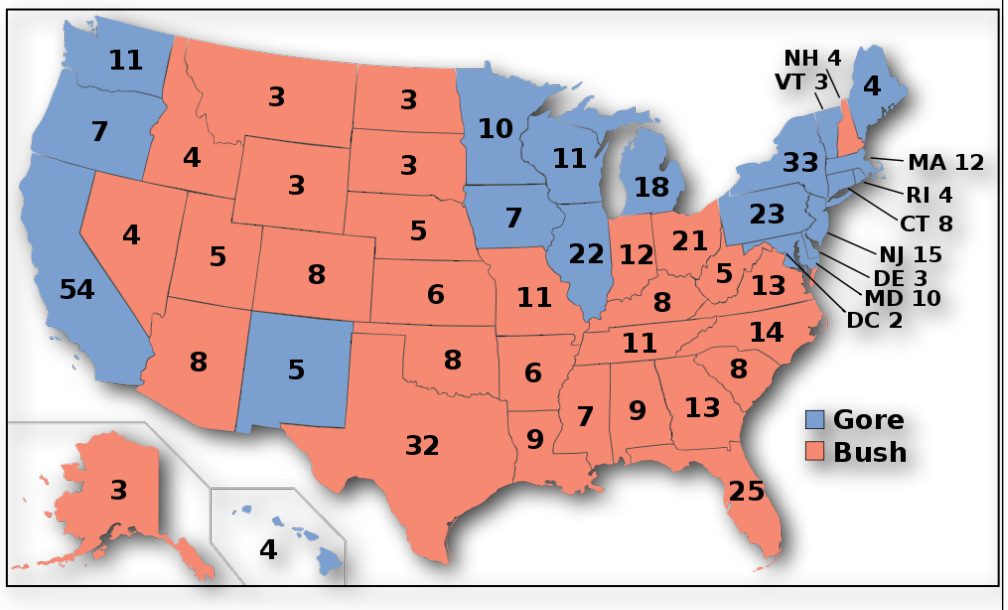


My Position on Evoting

- computers must not be used in the polling booth to record voter intent without paper ballots
- computers should only assist the disabled in exercising their right to a secret ballot
- computers may be used to assist in the creation and maintenance of voter lists, poll lists, and reporting results
- computers may be used to tally ballots, so long as risk-limiting post-election audits are used
- all technology used in an election must be Open Source, under public control, and rigorously treated as a safety-critical system

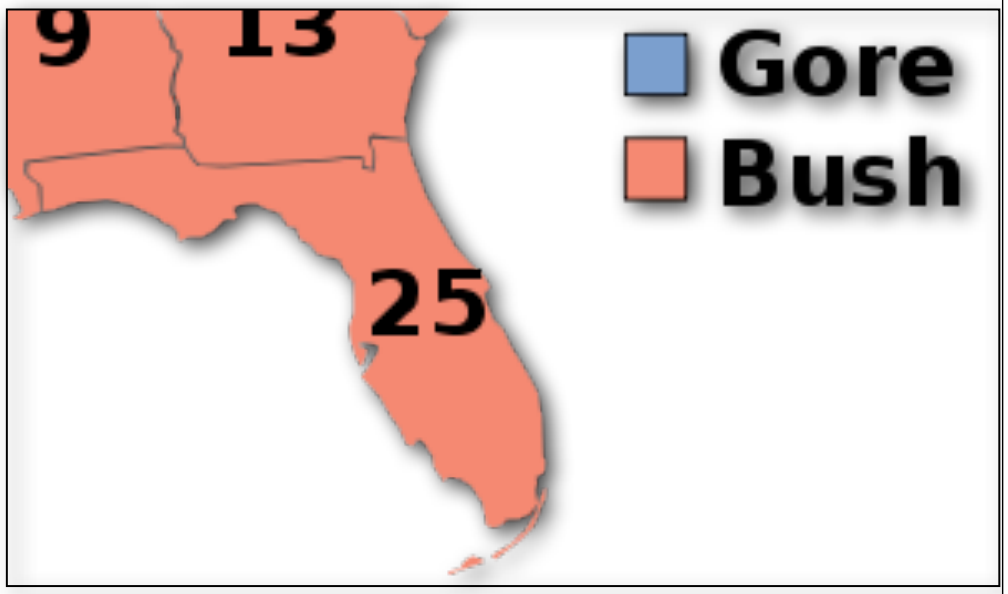
The 2000 U.S. Election

- extremely close race
- Florida the key state
- voting in the U.S.A.
- margin of victory
- spoiled ballots



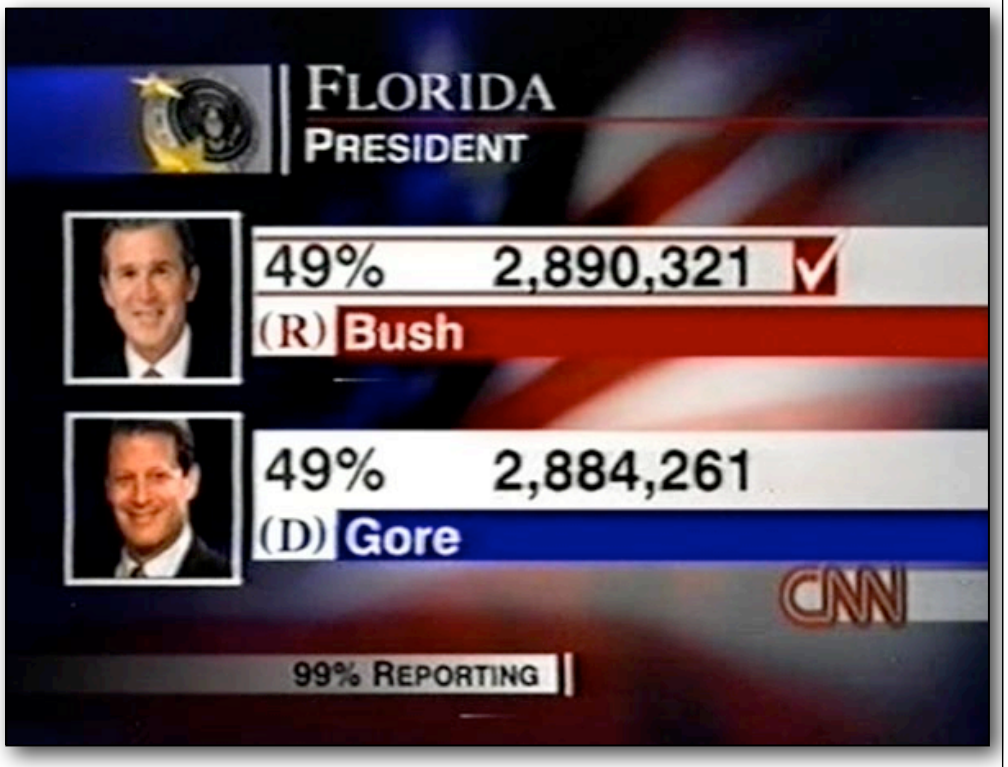
The 2000 U.S. Election

- extremely close race
- Florida the key state
- voting in the U.S.A.
- margin of victory
- spoiled ballots



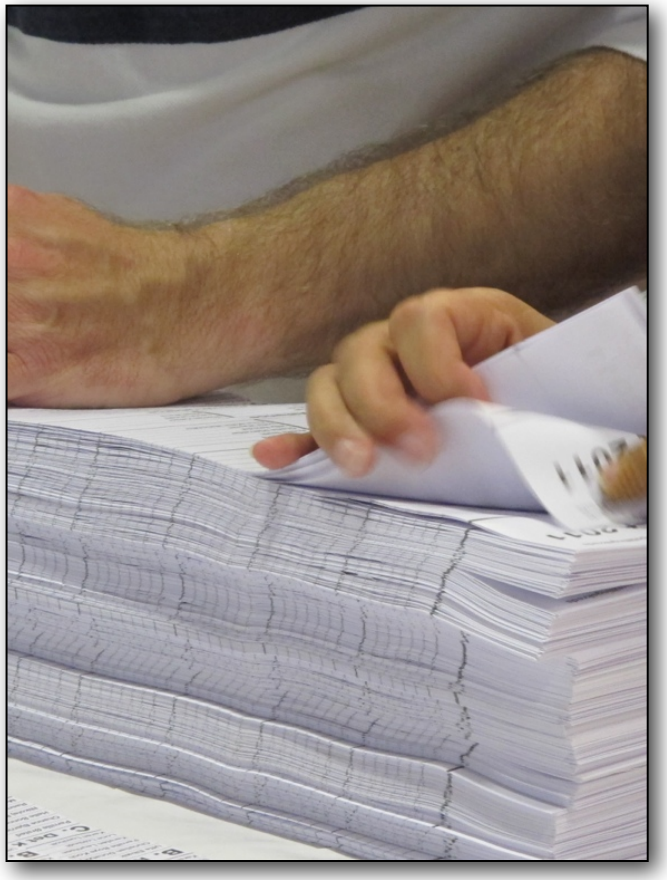
The 2000 U.S. Election

- extremely close race
- Florida the key state
- voting in the U.S.A.
- margin of victory
- spoiled ballots



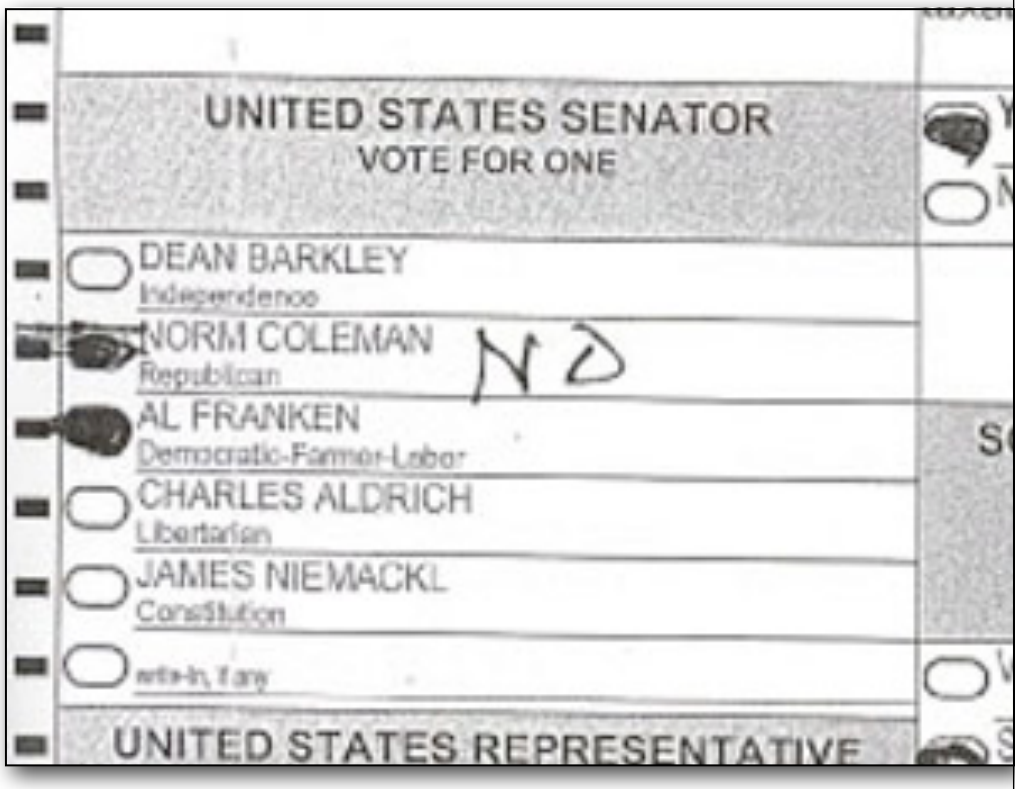
The 2000 U.S. Election

- extremely close race
- Florida the key state
- voting in the U.S.A.
- margin of victory
- spoiled ballots



The 2000 U.S. Election

- extremely close race
- Florida the key state
- voting in the U.S.A.
- margin of victory
- spoiled ballots



The 2000 U.S. Election

- extremely close race
- Florida the key state
- voting in the U.S.A.
- margin of victory
- spoiled ballots

Elections are Different

- enormous industry influence in government
- elections are fundamentally different than secure computer-based activities like banking
  - no equivalent of receipts or bank statement
- simultaneously ensuring all primary principles of secrecy, anonymity, coercion resistance, and verifiability is extremely difficult

Elections are finely-tuned algorithms where the computers are people.

DemTech

- Our question: *It is possible to modernize the electoral process while balancing the trust of the people on the trustworthiness of the deployed technology?*
- collaboration with Copenhagen, Aarhus, and Frederiksberg Municipalities
- originally in collaboration with Siemens and Aion via Assembly Voting; now forming Open Industrial Consortium
- official public experts for Ministry of the Economy and Interior via the Head of Elections
- all research and development results are public and unencumbered by any patents or trademarks

DemTech Research

- mathematical models of elections via epistemic and higher-order logics and within mechanized logical frameworks
- homomorphic and functional cryptography
- ethnographic analysis of elections
- historical and comparative analysis of trust and election technologies
- rigorous open systems engineering via a trust-by-design methodology

Election Fundamentals

- we have been voting for thousands of years
- there are many electoral schemes
- election schemes, policies, and procedures have been fine-tuned for centuries
- elections are algorithms, run by people and communities, using physical artifacts to accurately and securely measure voter intent while maintaining the trust of the electorate

Introducing computers into elections is a fundamental change to democracy!

Essence of an Election

- for an election to be accurate, secure, and maintain the trust of the electorate, the public must be able to see and authenticate these four essential steps of an election:

1. *who can vote* (the voter list)
2. *who did vote* (the poll list)
3. *counting of the vote* (tallying)
4. *chain of custody* (of all election artifacts)

If any one of these parts is violated, then the election is not public, democratic, and valid!

Democratic Principles

- *universal suffrage*: everyone has the right to vote and stand for election
- *equal suffrage*: each voter has an equal voice
- *free suffrage*: the voter can vote as they choose, without coercion or undue influence
- *secrete suffrage*: the voter has the right to secrecy, and the state has the duty to protect that right
- *direct suffrage*: the ballots cast in an election directly determine who is elected

Any change in elections must respect these principles!

Recommendations

- there are several formal recommendations and reports on electronic voting from governments, researchers, and NGOs
  - VerifiedVoting, ACCURATE, Jones' work, the U.S. EAC-especially the work of NIST, the California Voter Foundation, the Caltech-MIT Voting Technology Project, the Diebold report, the SERVE report, the SAIC report, the RABA report
  - Council of Europe [CoE (2004)11]

CoE (2004)11 Contents

- 112 requirements, 191 detailed legal standards, and extensive technical security recommendations and risk analysis standards, including dozens of primary threats and their impact on the objectives of an election using evoting technology

1. legal standards for elections
2. procedural safeguards (transparency, verifiability and accountability, reliability and security)
3. operational standards (notification, voters, candidates, voting, results, audit)
4. technical requirements (accessibility, system operation, security)

Computers in Elections

- computer are in elections today, even in democracies with no visible machines in the polling booth
- voter lists computed and printed, intermediate results are transmitted and recorded digitally, final results are computed, often with Microsoft Excel

In countries that use computers to record voter intent in the polling booth or via the internet, there is no public control.

Evoting System Flavors

- bespoke low-tech voting systems
  - NL's Nedap, India's EVM
- optical mark-sense voting systems
  - electronic ballot markers & digital pens
- DRM (with or without paper audit trails)
- remote/internet voting systems
- end-to-end, voter-verifiable systems
  - Punchscan, Scantegrity I & II, Prêt à Voter

Bespoke Systems

- computers used in elections since the mid-1980s
- voting machines are simple computers
- 8 bit CPUs, minimal RAM and store, custom PCBs, no operating system

Bespoke Systems

- computers used in elections since the mid-1980s
- voting machines are simple computers
- 8 bit CPUs, minimal RAM and store, custom PCBs, no operating system

Bespoke Systems

- computers used in elections since the mid-1980s
- voting machines are simple computers
- 8 bit CPUs, minimal RAM and store, custom PCBs, no operating system

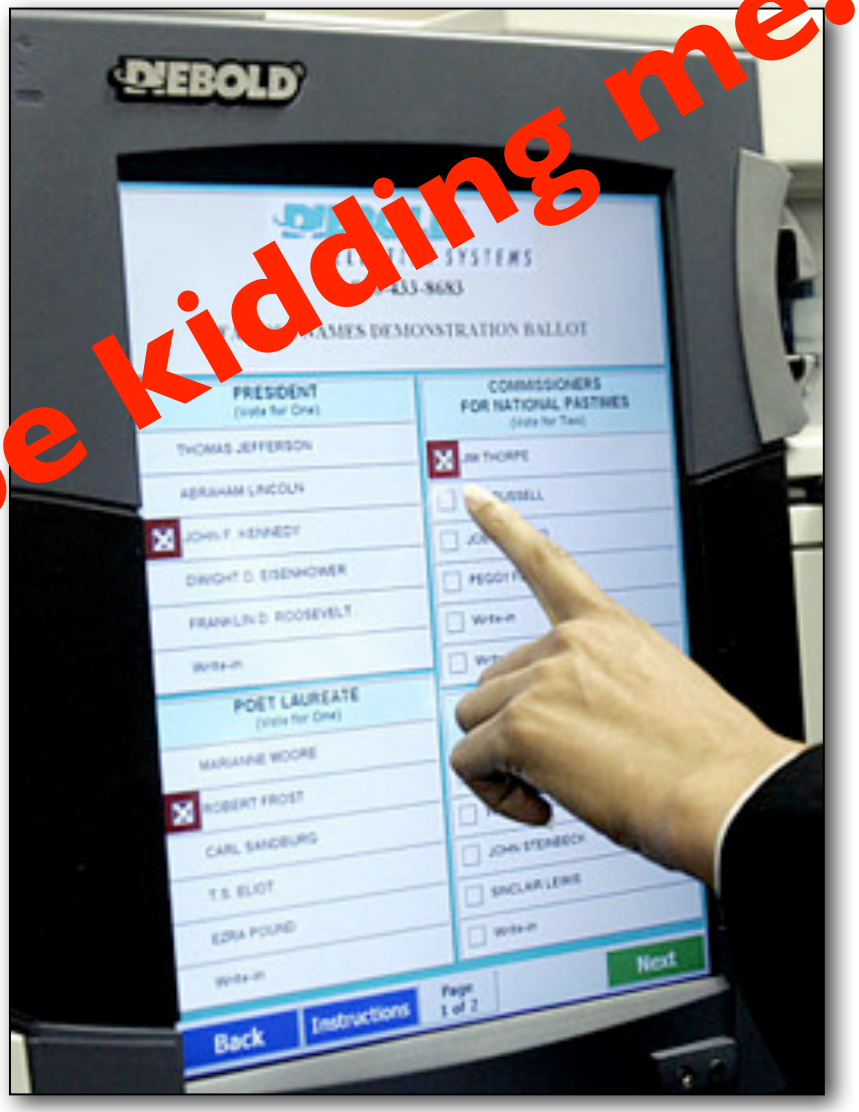
Optical Scanners

Typical DRM Machine

- terribly built
- runs Windows
- uses commodity hardware
- no paper ballots
- voter must trust that it works correctly

Typical DRM Machine

- terribly built
- runs Windows
- uses commodity hardware
- no paper ballots
- voter must trust that it works correctly



You have to be kidding me!

Internet Voting Systems

- experiments conducted in several countries
- rejected in most countries due to conflict with fundamental principles of democracy
- experiments we are most familiar with are those of Holland and Norway

The systems we have analyzed have many serious system design and engineering problems and violate free and secret suffrage.

E2E Voter-Verifiable Systems

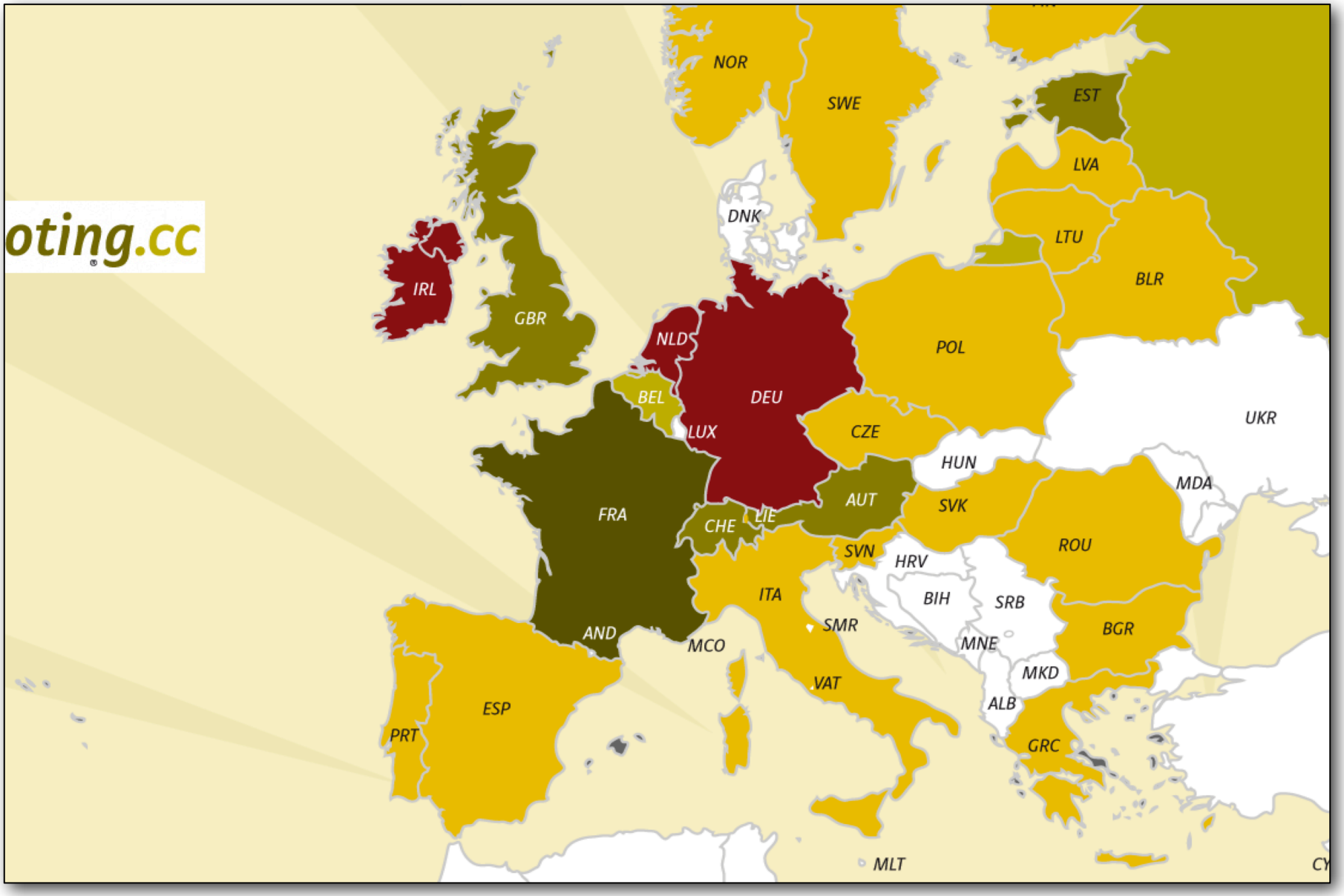
- dramatically or subtly change the manner in which one votes
  - e.g., tearing ballot or invisible ink
- advanced cryptography used to guarantee post-election voter-verifiability

Incomprehensible to virtually all citizens.

State-of-the-Art Assessment

- personally assessed many evoting software systems (commercial and research) and read reports on hardware systems
- these systems, in the general, have
  - poor software engineering practices
  - no rigorous validation and verification
  - little traceability to requirements
  - questionable certification
  - poor quality and security

Evoting in Europe



The Netherlands

- unofficial and then official security audits
- Parliament report
- rigorously engineered tallying system
- colleagues were hacking machines
- evoting banned

Ireland

- Nedap machines purchased hours before e-voting experts scheduled to report to government committee
- not asked back to subcommittee of CEV for asking the wrong questions
- advised team to check the correctness of the tally system
- supervised development of rigorously engineering tally system for Ireland's PR-STV election scheme
- evoting banned

U.S.A.

- Help America Vote Act (HAVA)
- forced municipalities to quickly buy election equipment with...
  - no vetting
  - little support for certification
  - no funding for long-term support
- election equipment certification guarantees hardiness, not correctness or security

Lessons Learned

- do not permit vendors to lead government
- listen to experts, or suffer the consequences
- do not permit one vendor to design, build, manage, and run elections
- all hardware and software relating to elections must be public (Open Source)

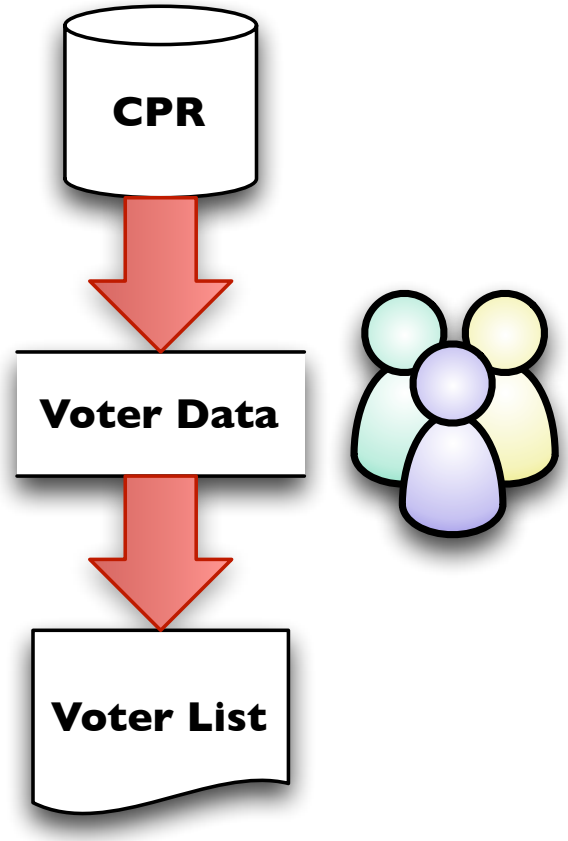
Public control of the entire election apparatus and preserving the trust of the electorate is of paramount importance!

Danish Elections Today

- DemTech were election observers for the 2011 elections
- we had people in the field at Municipality offices and in polling stations full time
- full access to election officials, relevant documents, policies, and procedures
- observed rough counts in several locations
- observed the fine count
- were excused during the final tallying

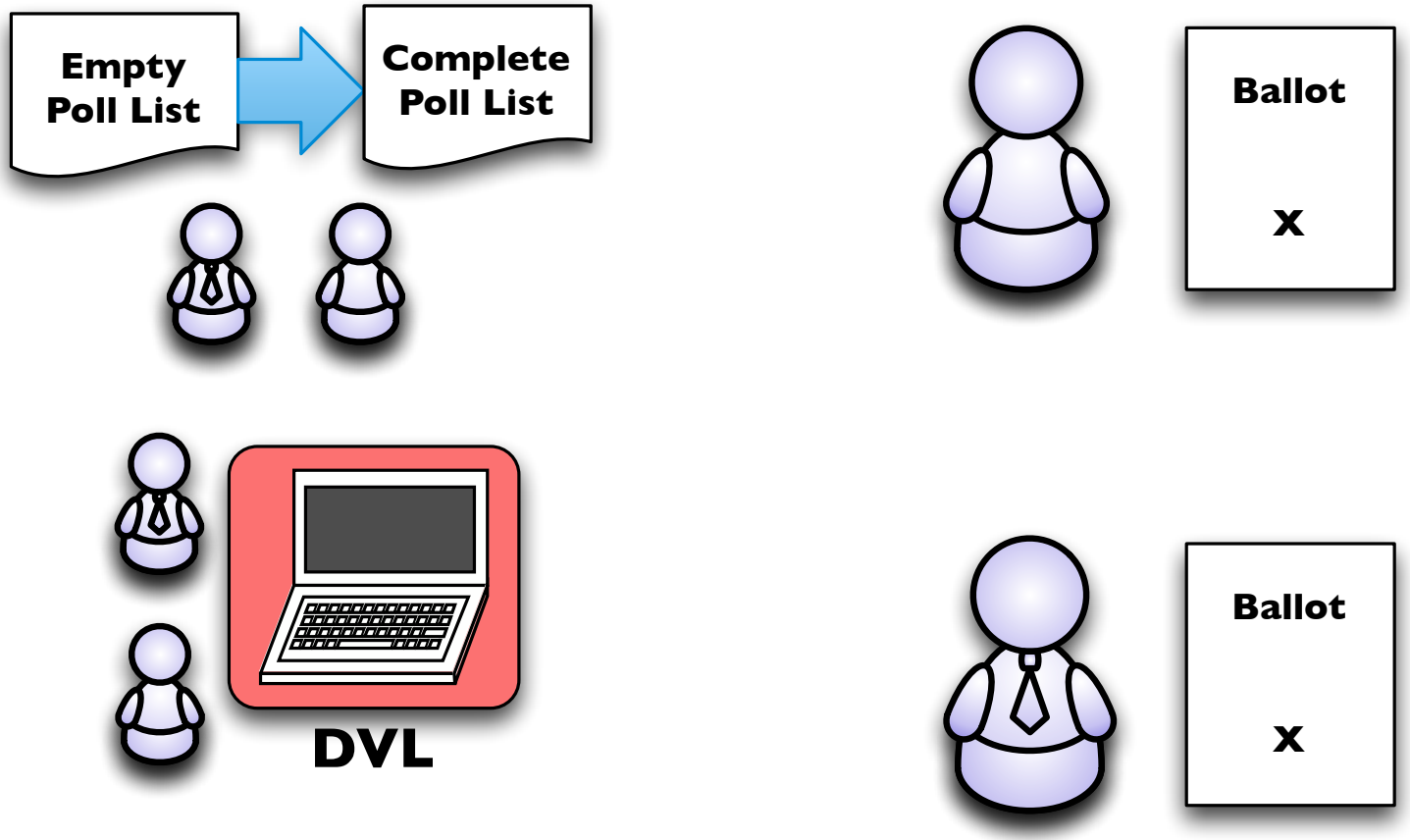
DK Elections Today

Pre-election



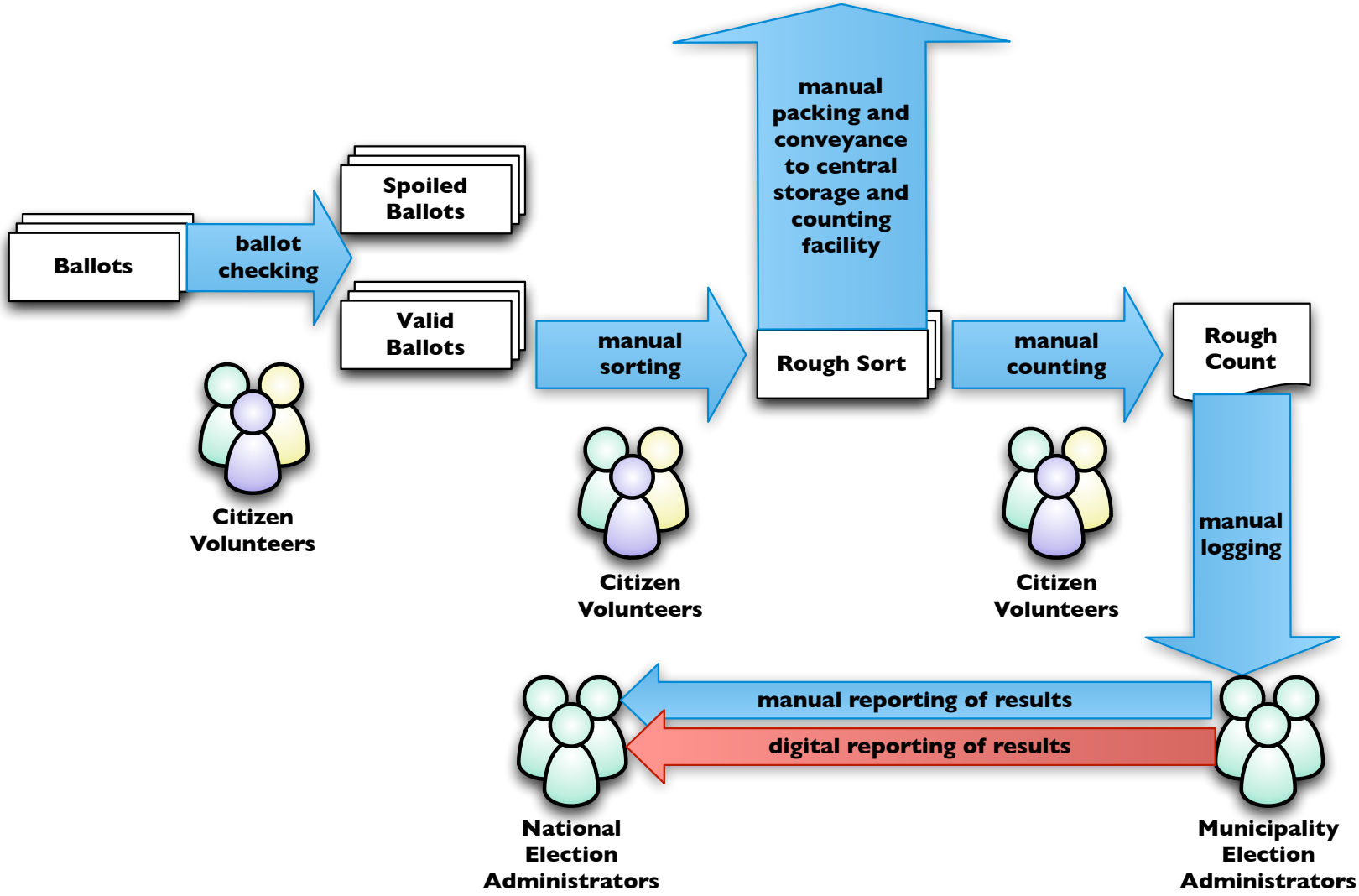
DK Elections Today

Election Day: Polls are Open



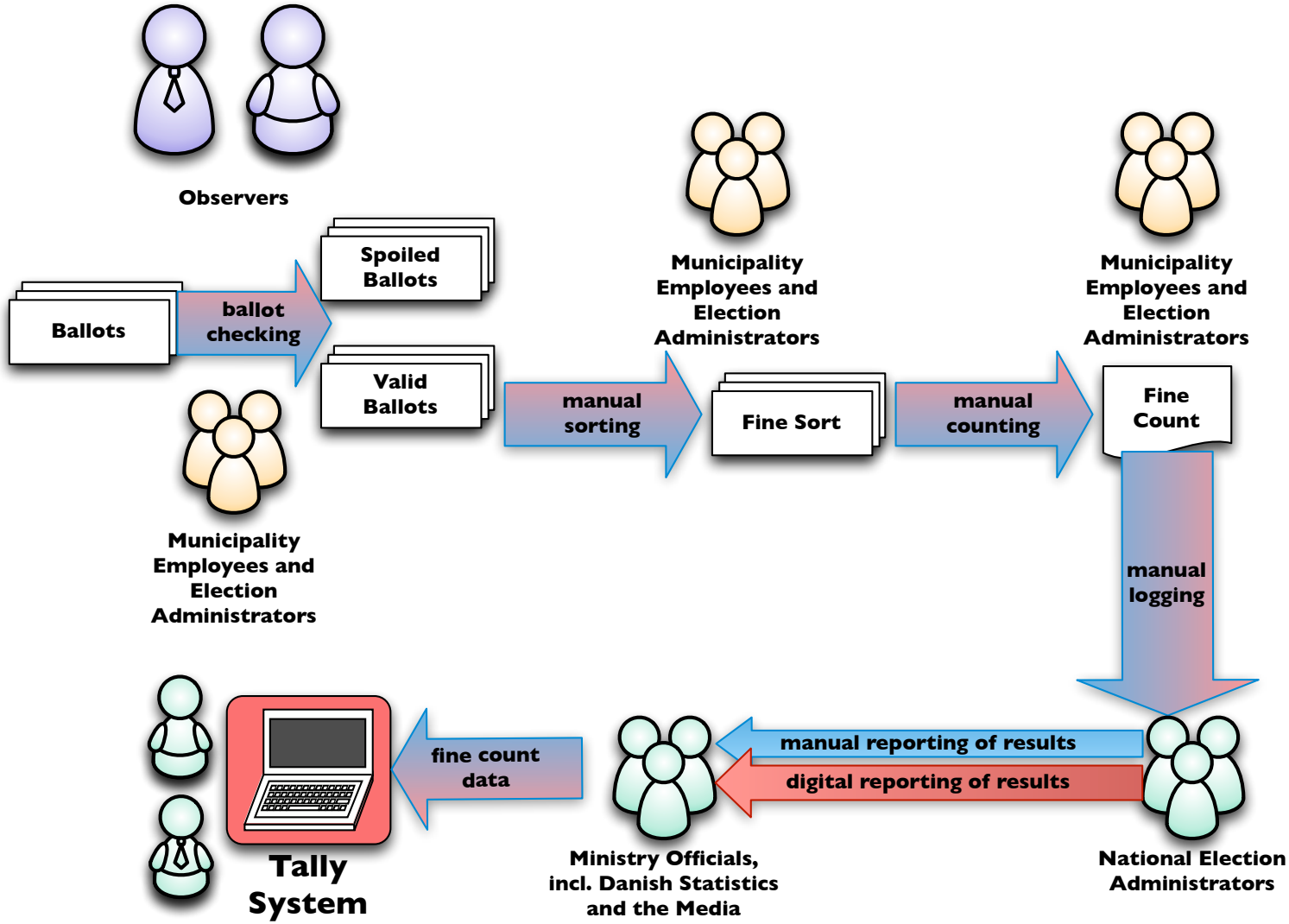
DK Elections Today

Election Day: Polls are Closed (The "Rough" Count)



DK Elections Today

Post-Election Day: The "Fine" Count and Reporting



Denmark Tomorrow

- what will elections look like during trials?
- what might they look like in the future, if we follow the path of other countries?
- what might they look like in the future if we realize Open Source Elections?

Denmark Tomorrow

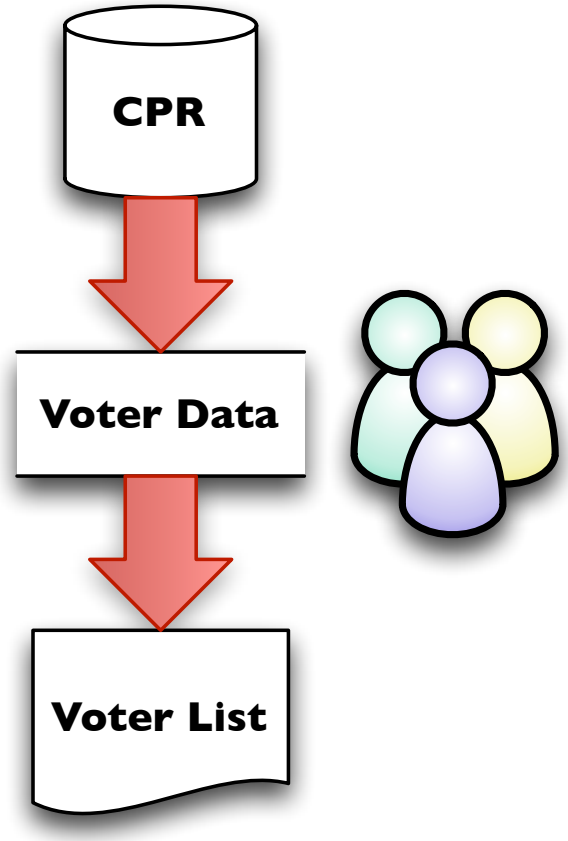
- *what will elections look like during trials?*
- what might they look like in the future, if we follow the path of other countries?
- what might they look like in the future if we realize Open Source Elections?

Draft Law (L132)

- permit binding trials in the use of computers in supervised voting
- stated reasons for proposed change
  - increase accessibility for the disabled
  - increase the accuracy & speed of tallying
  - minimizing accidental invalid votes
  - potentially decrease costs in the long run

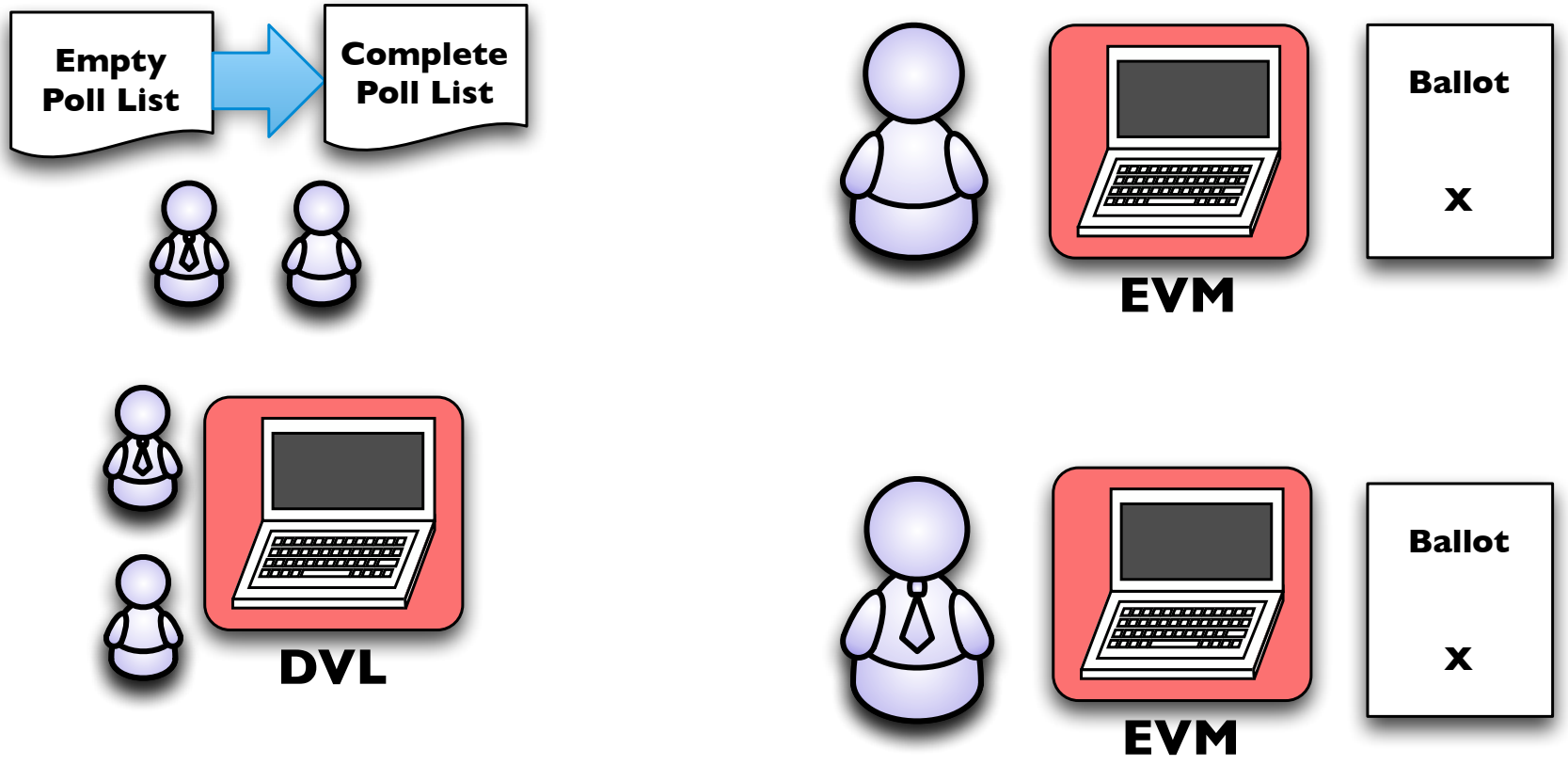
DK Elections During Trials

Pre-election



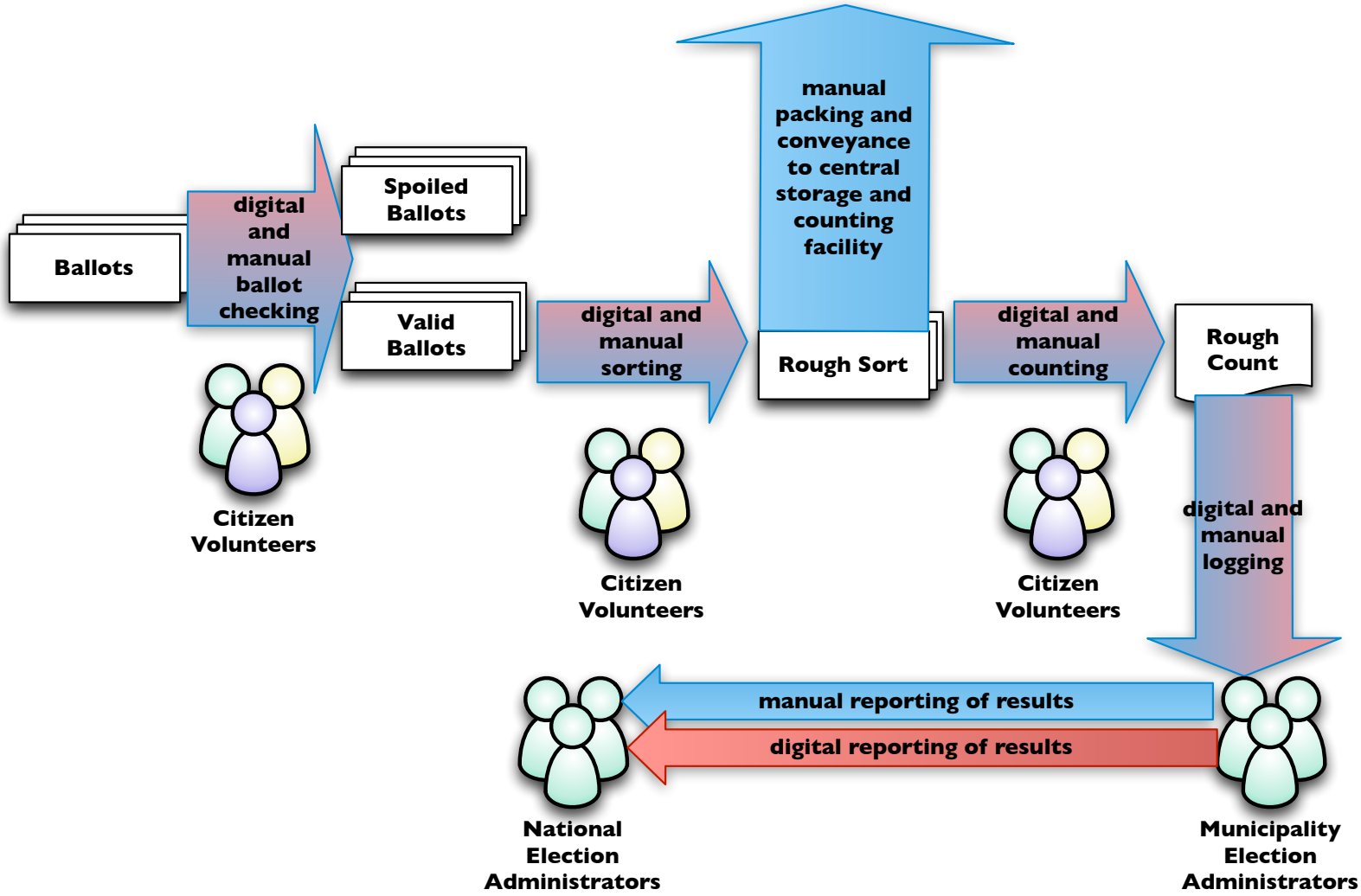
DK Elections During Trials

Election Day: Polls are Open



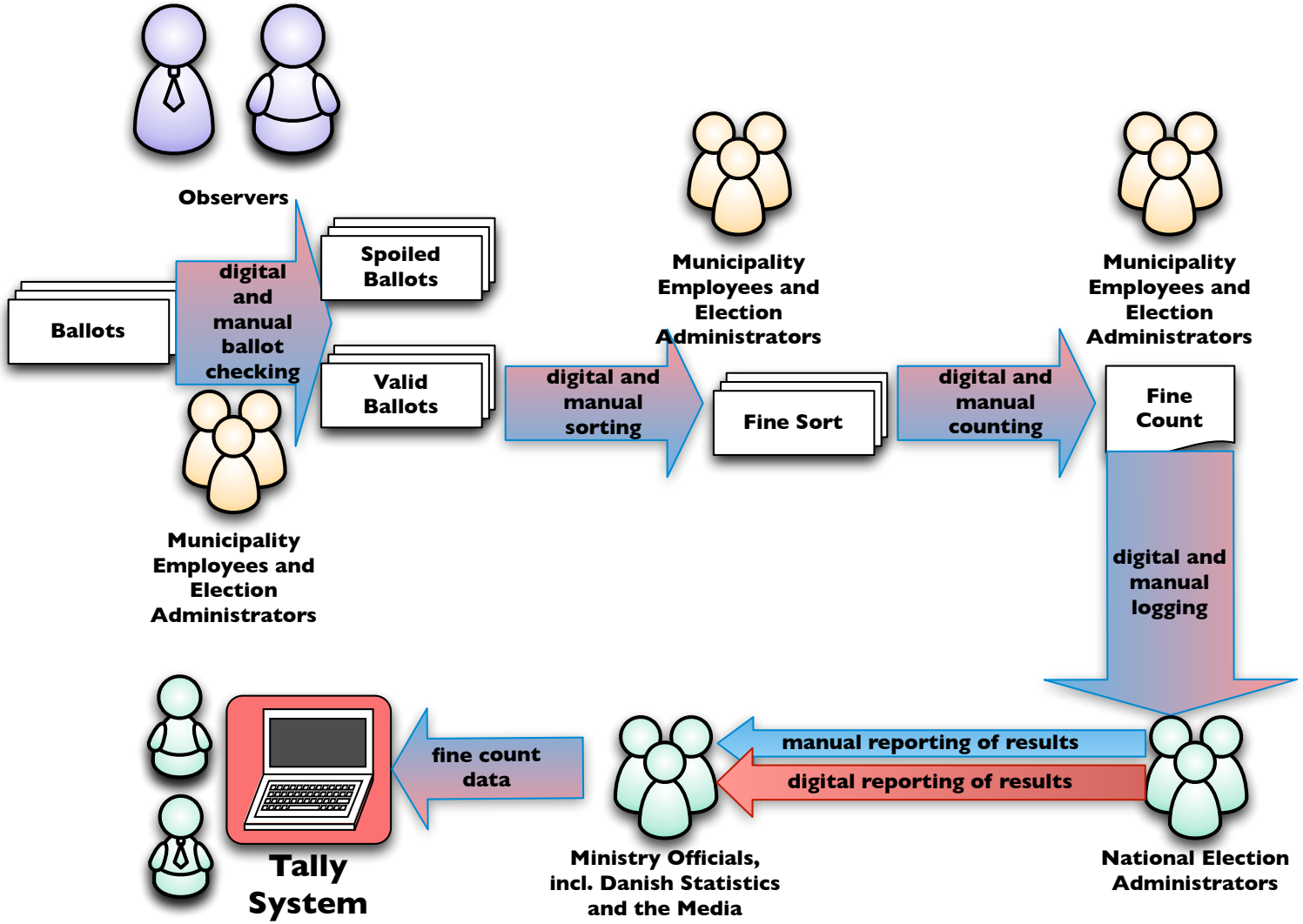
DK Elections During Trials

Election Day: Polls are Closed (The "Rough" Count)



DK Elections During Trials

Post-Election Day: The "Fine" Count and Reporting



Consultation Responses

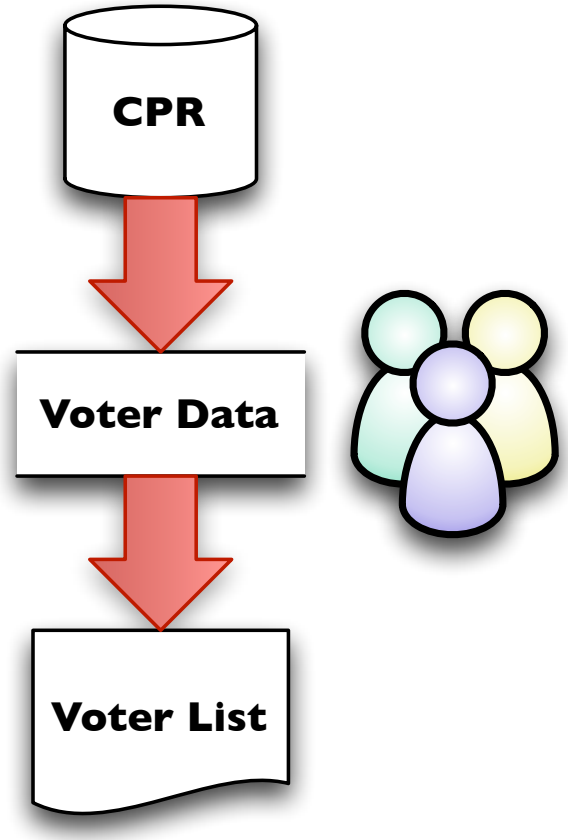
- DFS, Danish Disability Organizations, Danish Regions, DUF, ITU/DemTech, DI-ITEK, and DIKU positive to cautiously positive about the notion of conducting trials (some with significant strong recommendations)
- independent IT experts and various political science organizations and departments are critical in proposed change in law and recommend rejection
- first hearing for the draft law is next Thursday the 7th of February

Denmark Tomorrow

- what will elections look like during trials?
- *what might they look like in the future, if we follow the path of other countries?*
- what might they look like in the future if we realize Open Source Elections?

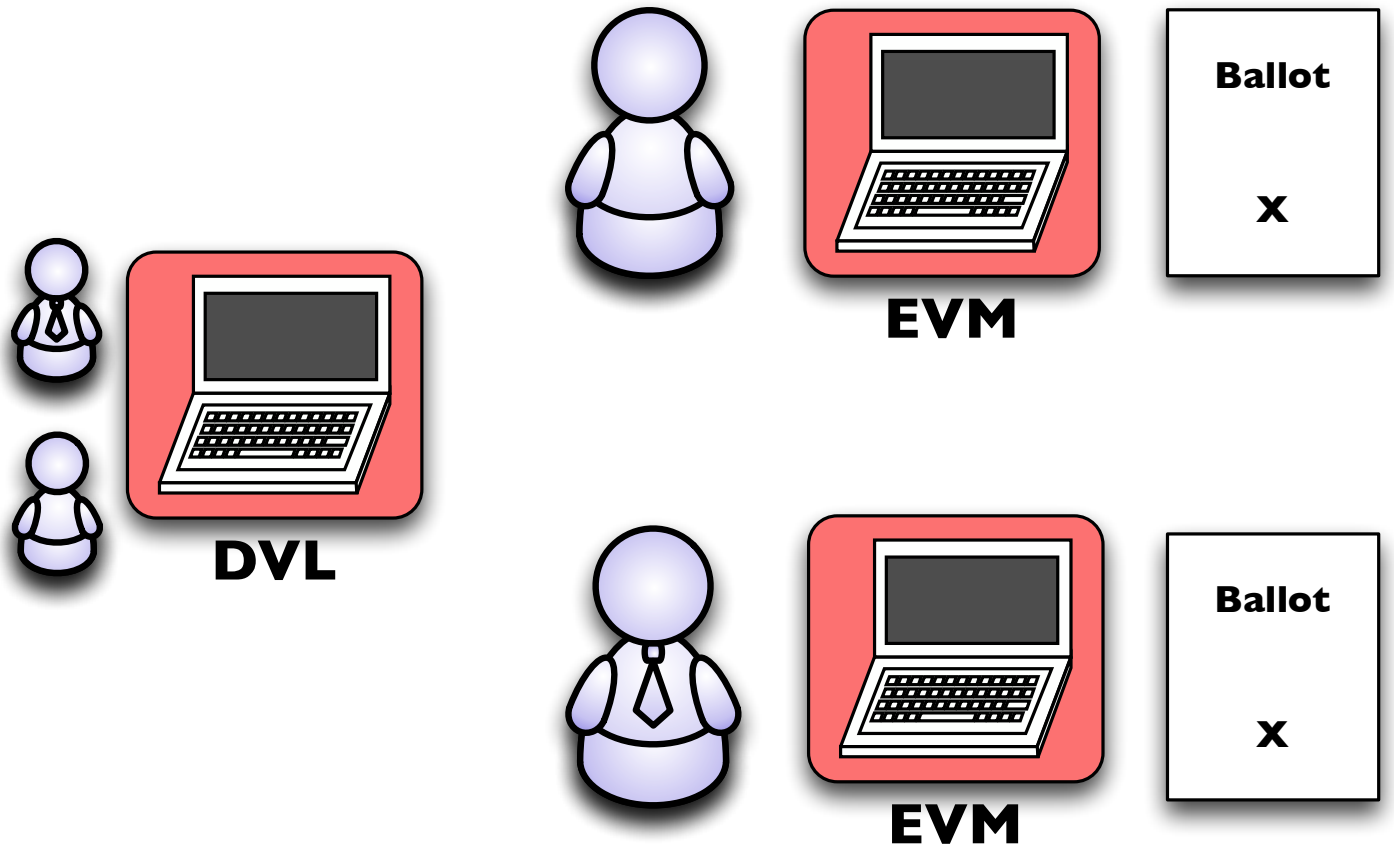
DK Elections Future?

Pre-election



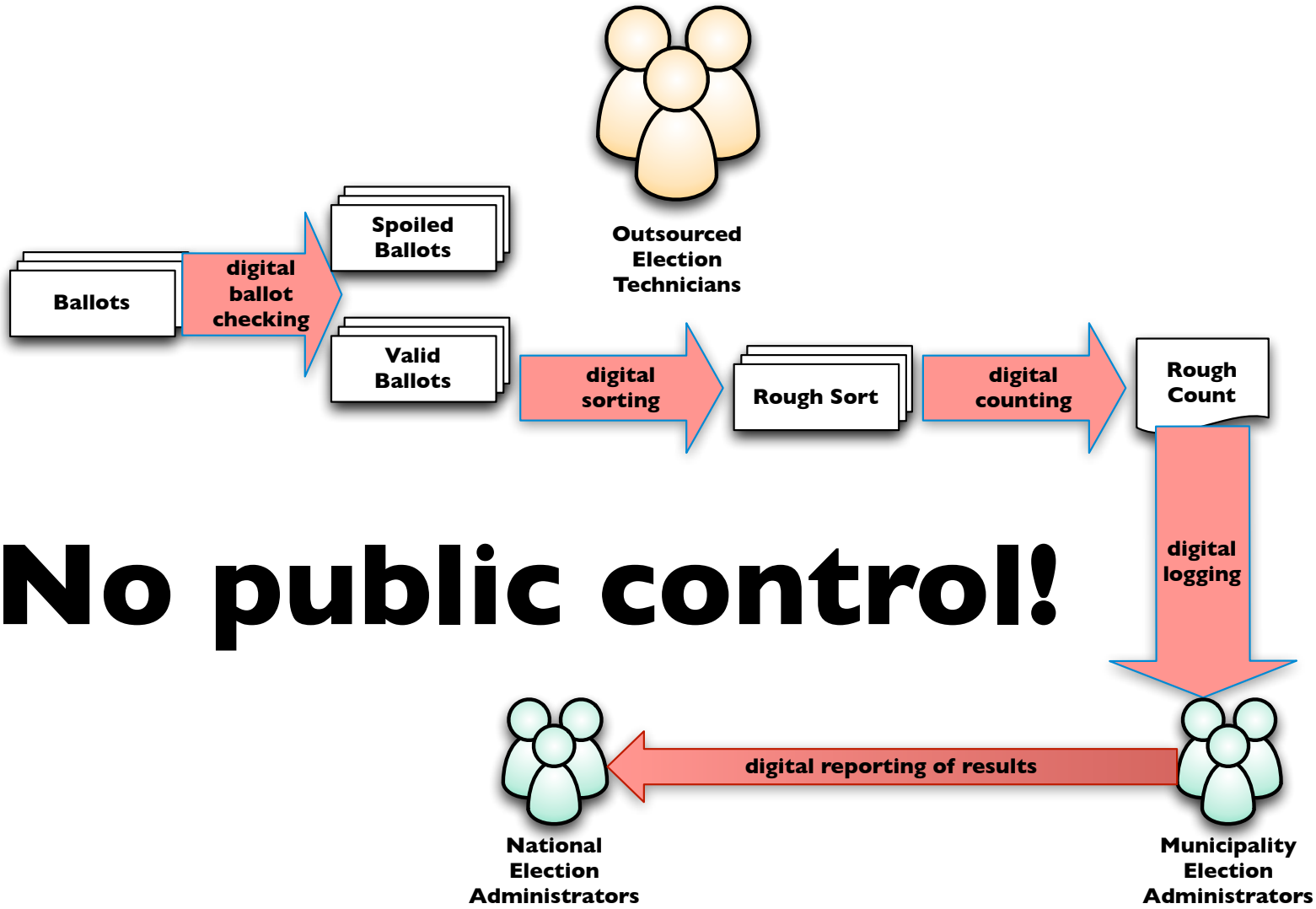
DK Elections Future?

Election Day: Polls are Open



DK Elections Future?

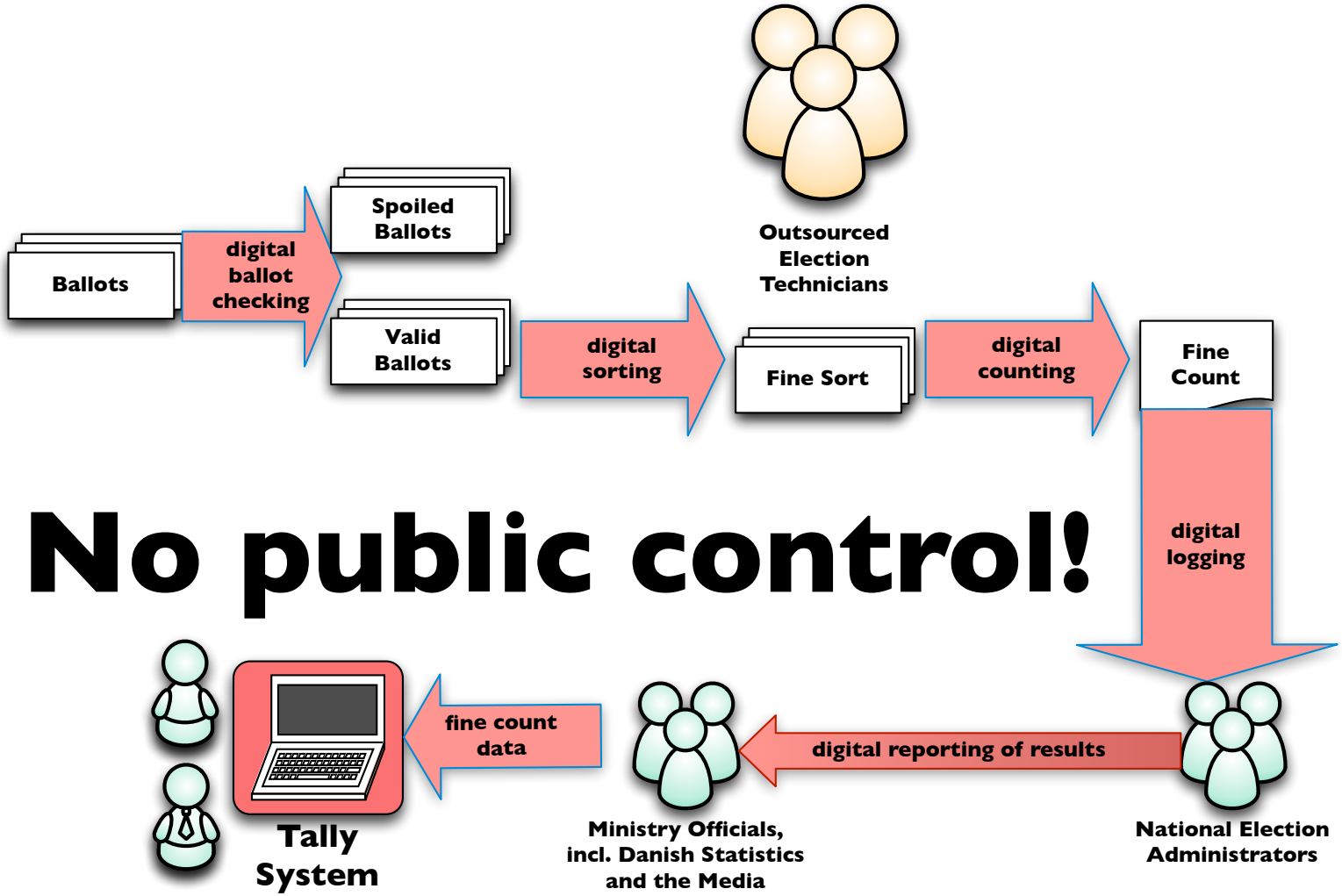
Election Day: Polls are Closed (The "Rough" Count)



No public control!

DK Elections Future?

Post-Election Day: The "Fine" Count and Reporting

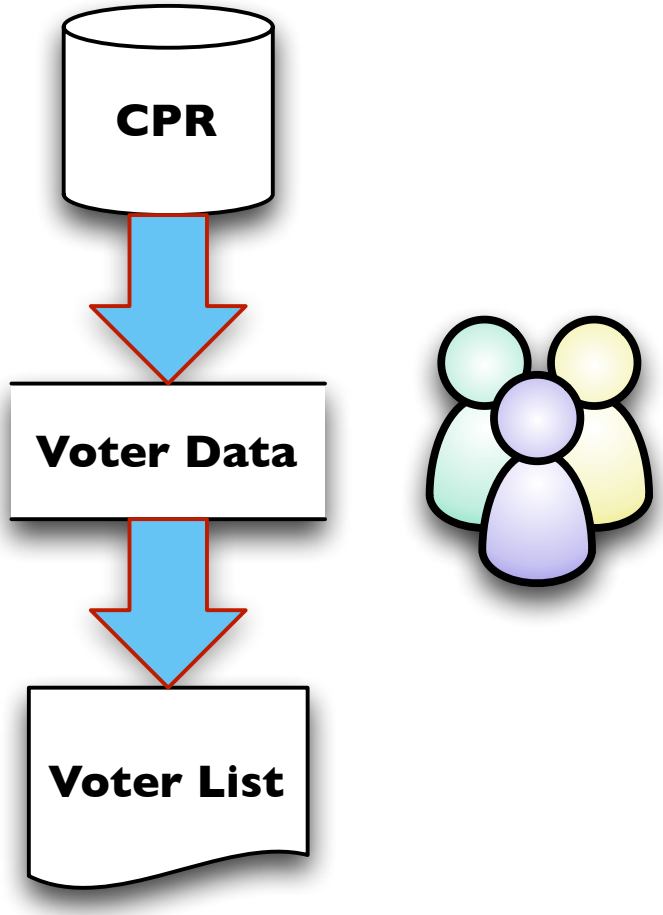


Denmark Tomorrow

- what will elections look like during trials?
- what might they look like in the future, if we follow the path of other countries?
- *what might they look like in the future if we realize Open Source Elections?*

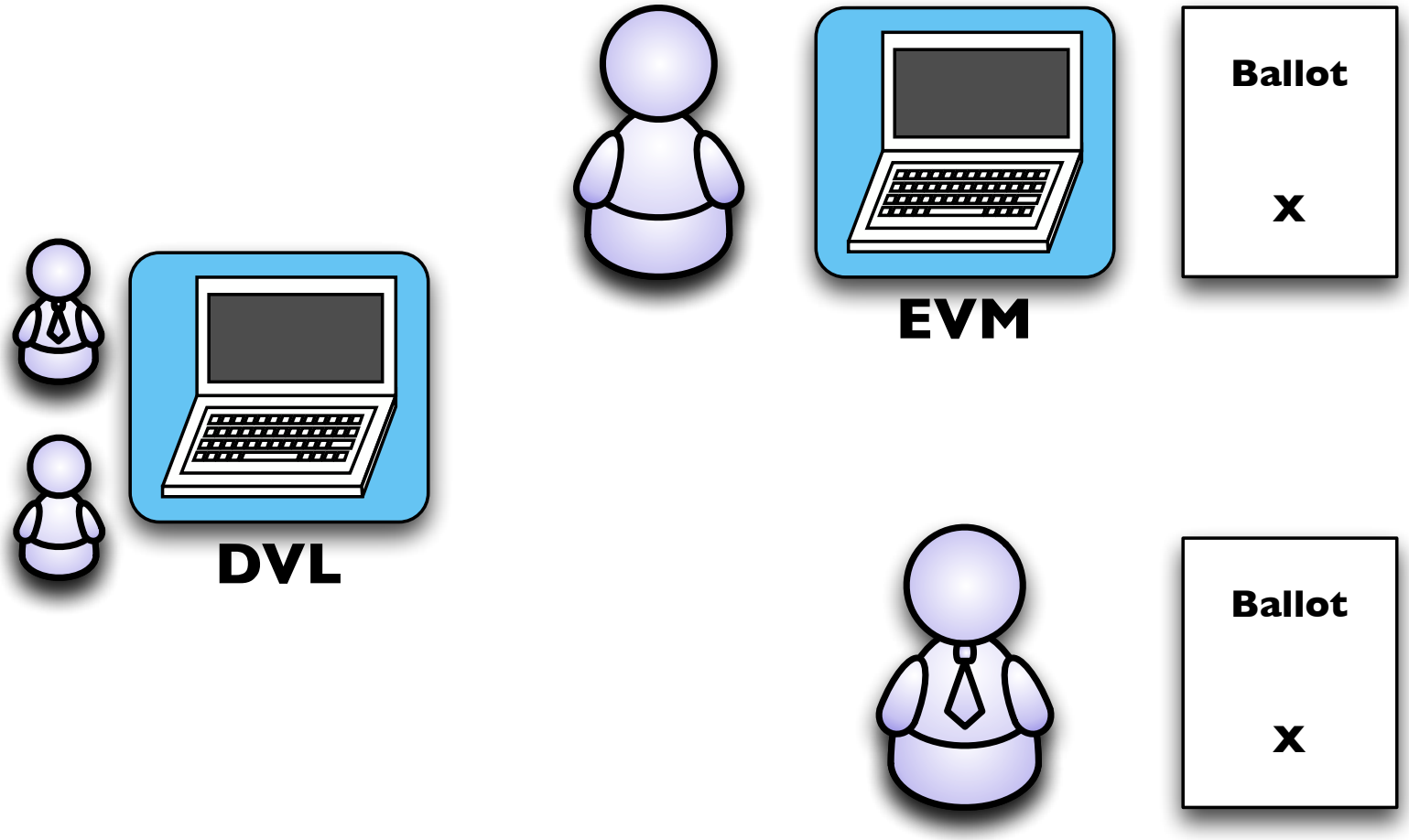
DK Open Source Elections

Pre-election



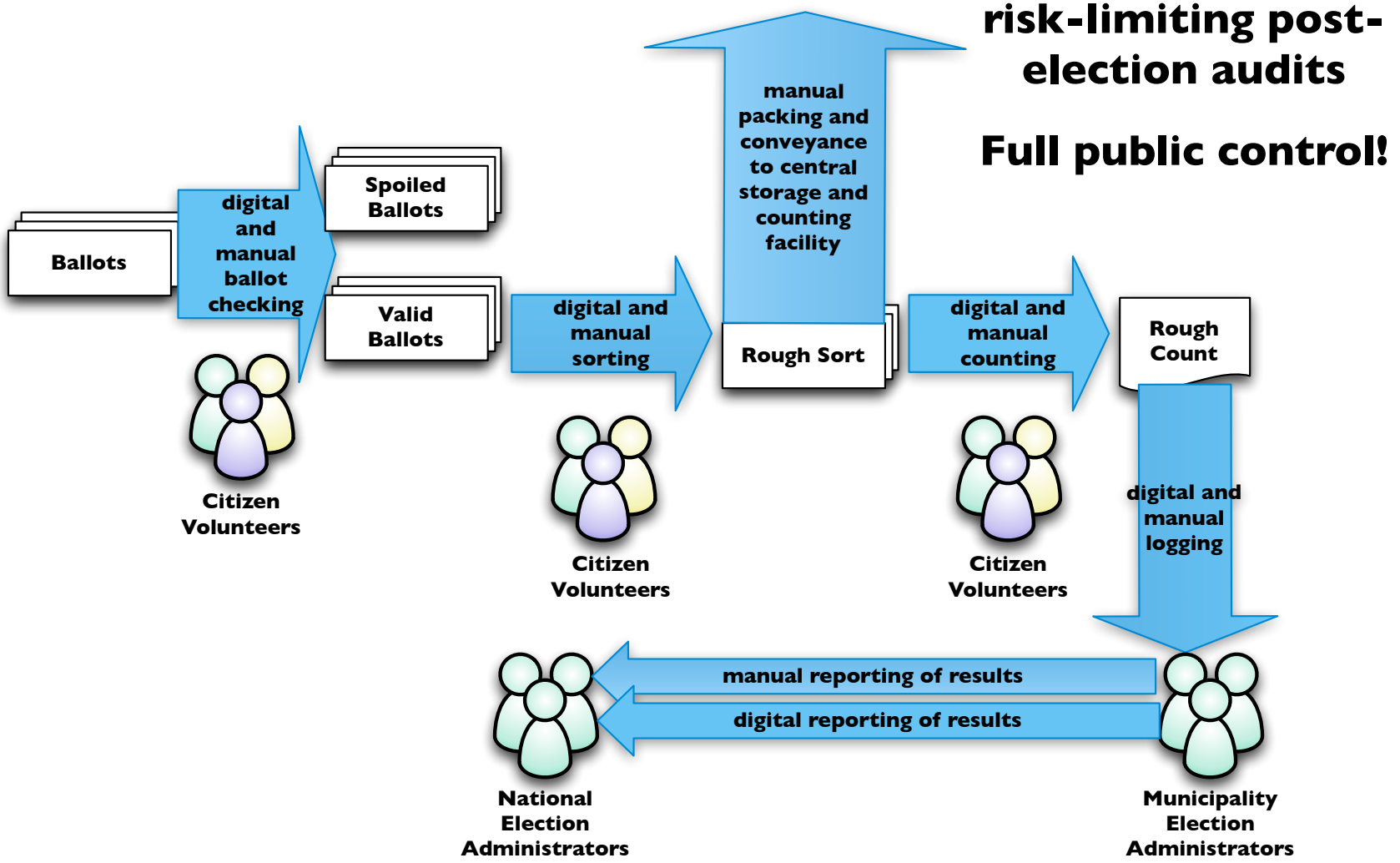
DK Open Source Elections

Election Day: Polls are Open



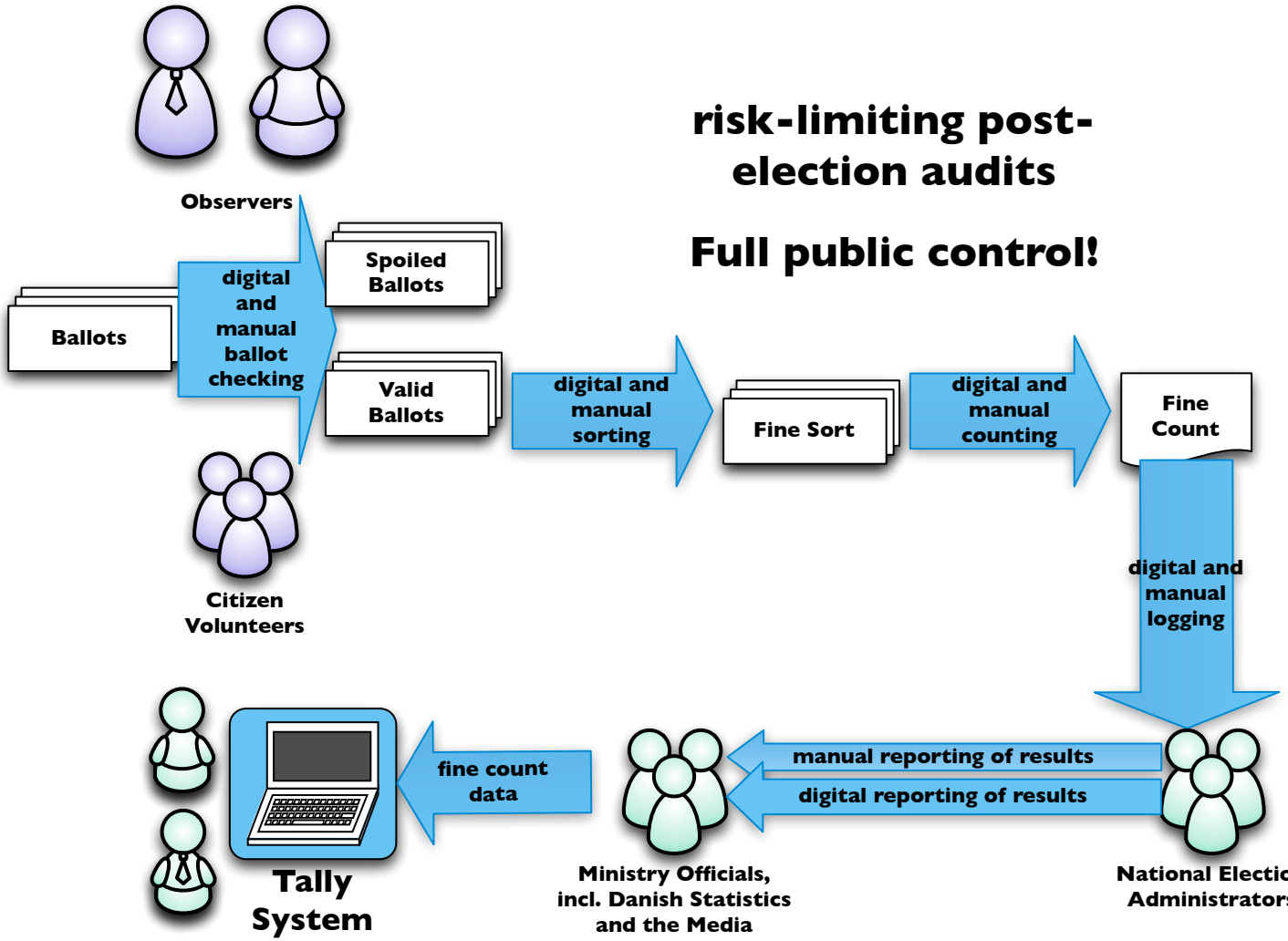
DK Open Source Elections

Election Day: Polls are Closed (The "Rough" Count)



DK Open Source Elections

Post-Election Day: The "Fine" Count and Reporting



Research Opportunities

- treat elections as system engineering
  - make recommendations to change processes by technical analysis, rather than introducing technology
  - information security principles to analyze elections for insider and outsider attack

Elections as Algorithms

- view the election apparatus as a distributed system, with humans as the computers, and ballots and numbers are the data
- use queueing theory and simulation to optimize polling place organization
- use protocol design and analysis and error-correcting codes to tune manual reporting
- use interface and interactive design principles to improve ballot design
  - e.g., add a box in which voters put an 'X'

Optimizing Algorithms

- at its core, the expensive part of manual elections are the sorting and counting algorithms
- the rough and fine count stages are concurrent systems
- use simulation and algorithm analysis to optimize manual sorting and counting
  - move from ad hoc sorting to better concurrent algorithm in this context
  - e.g., weigh ballot paper stacks, rather than manually count them

Denmark Tomorrow?

- let's not repeat others' expensive and embarrassing mistakes
- trillions of dkk in the U.S.A.
- hundreds of millions dkk in NL
- 500M dkk in Ireland
- loss of trust in the electorate

Final Recommendation

- *reject the proposed change in law and let DemTech do their job through 2015*
  - develop rigorously engineered Open Source technologies to replace and augment all existing proprietary, expensive technologies
    - voter list, ballot printer, logging, tallying
  - analyze and optimize existing manual election procedures to increase accuracy and security and decrease cost of current elections
- *at that time, reassess based upon the objective scientific evidence and the trust of the electorate*