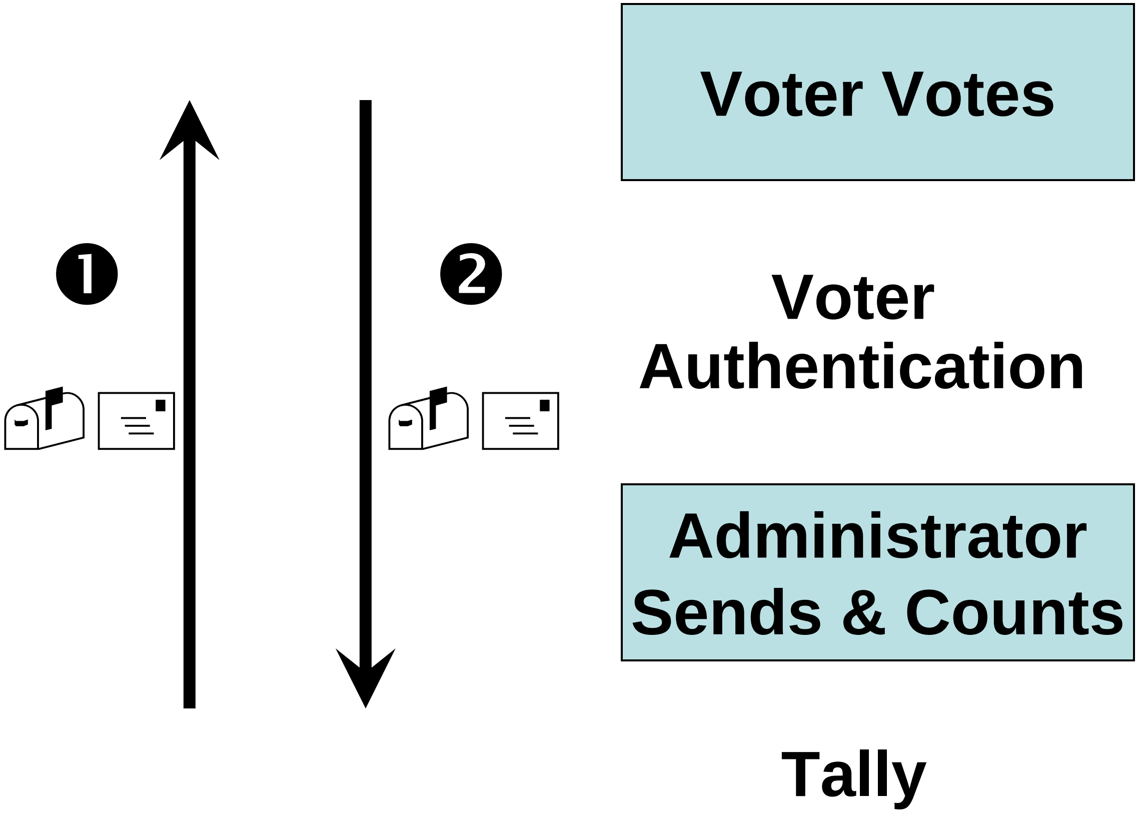
# PunchScan for Remote Board Elections

David Chaum, Stefan Popoveniuc

(Richard Carback, Jeremy Clark, Aleks Essex)

# Typical Current System



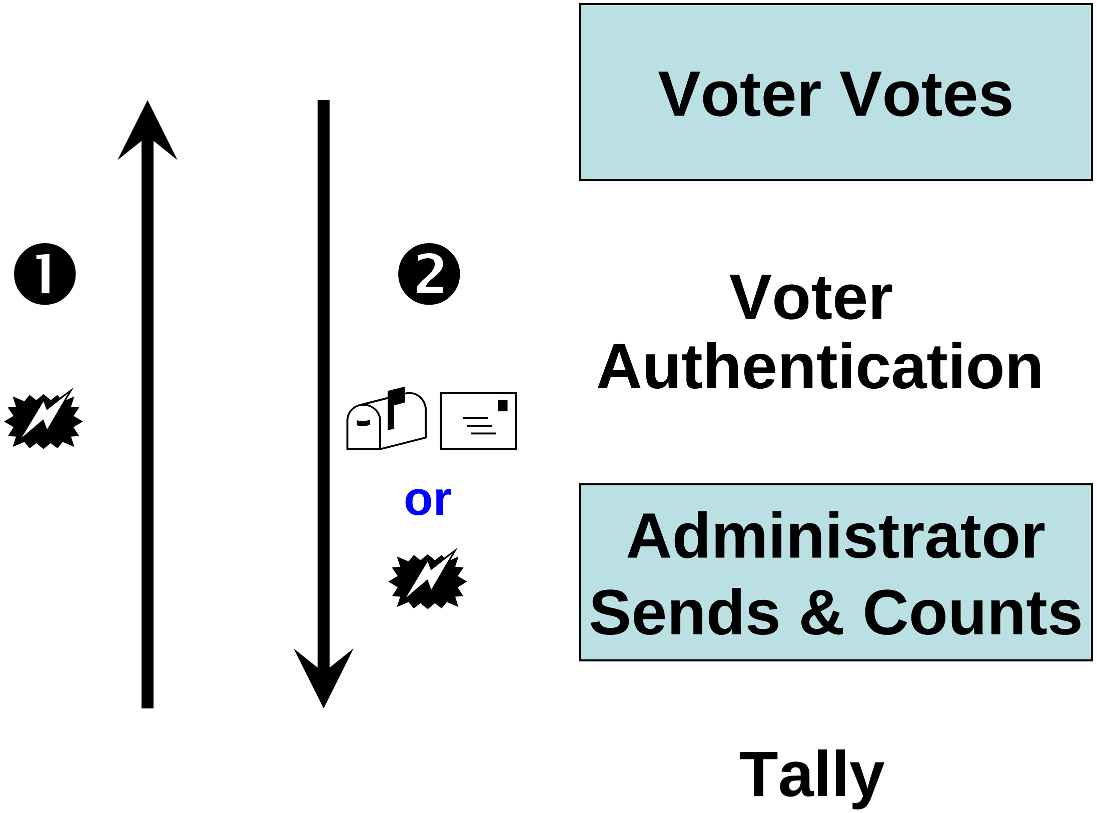
Voter Votes

Voter Authentication

Administrator Sends & Counts

Tally

# Adding Electronic Communication



Voter Votes

❶

❷

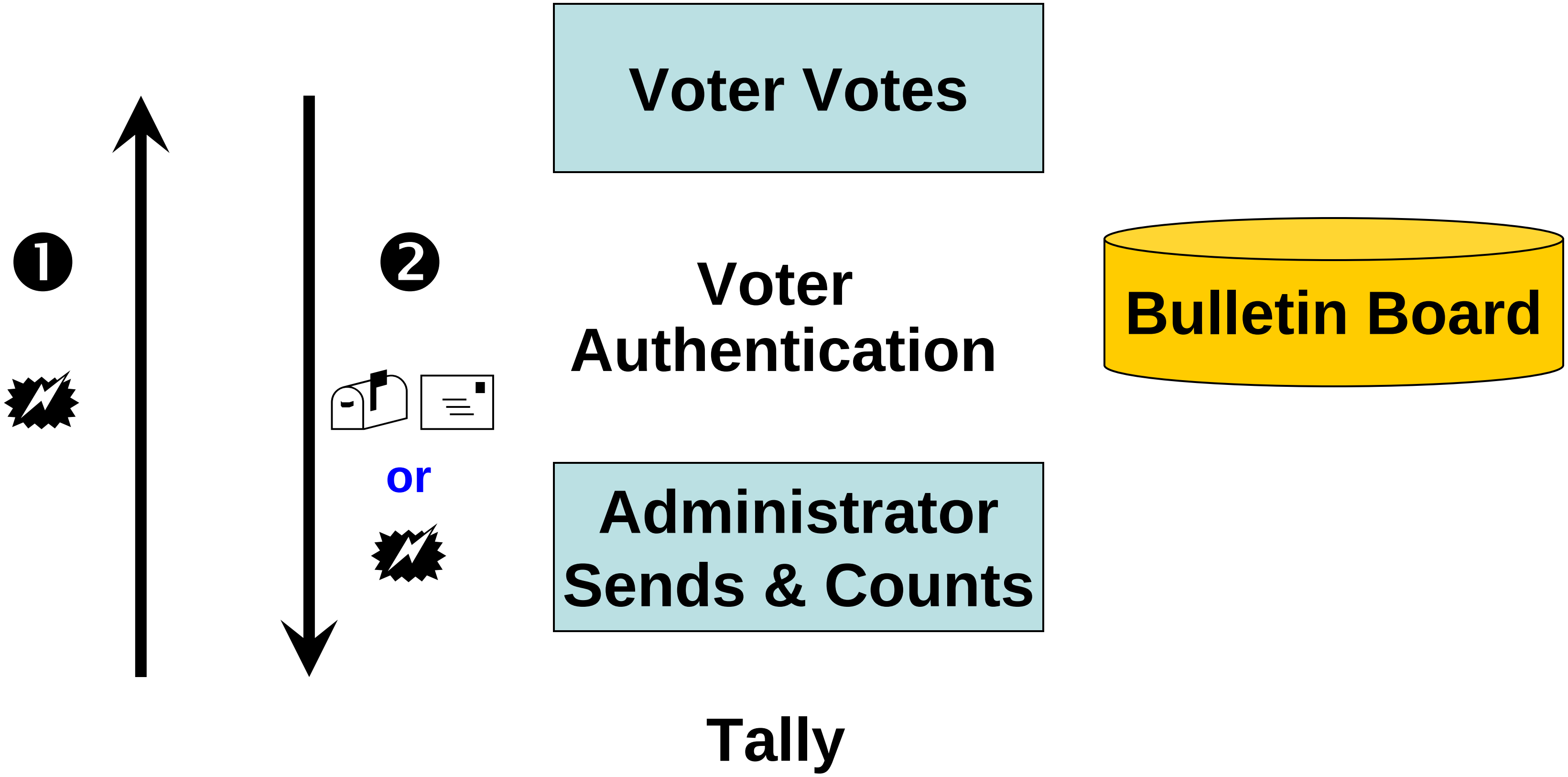
Voter Authentication

or

Administrator Sends & Counts

Tally

# Adding a Bulletin Board



❶

❷

or

Voter Votes

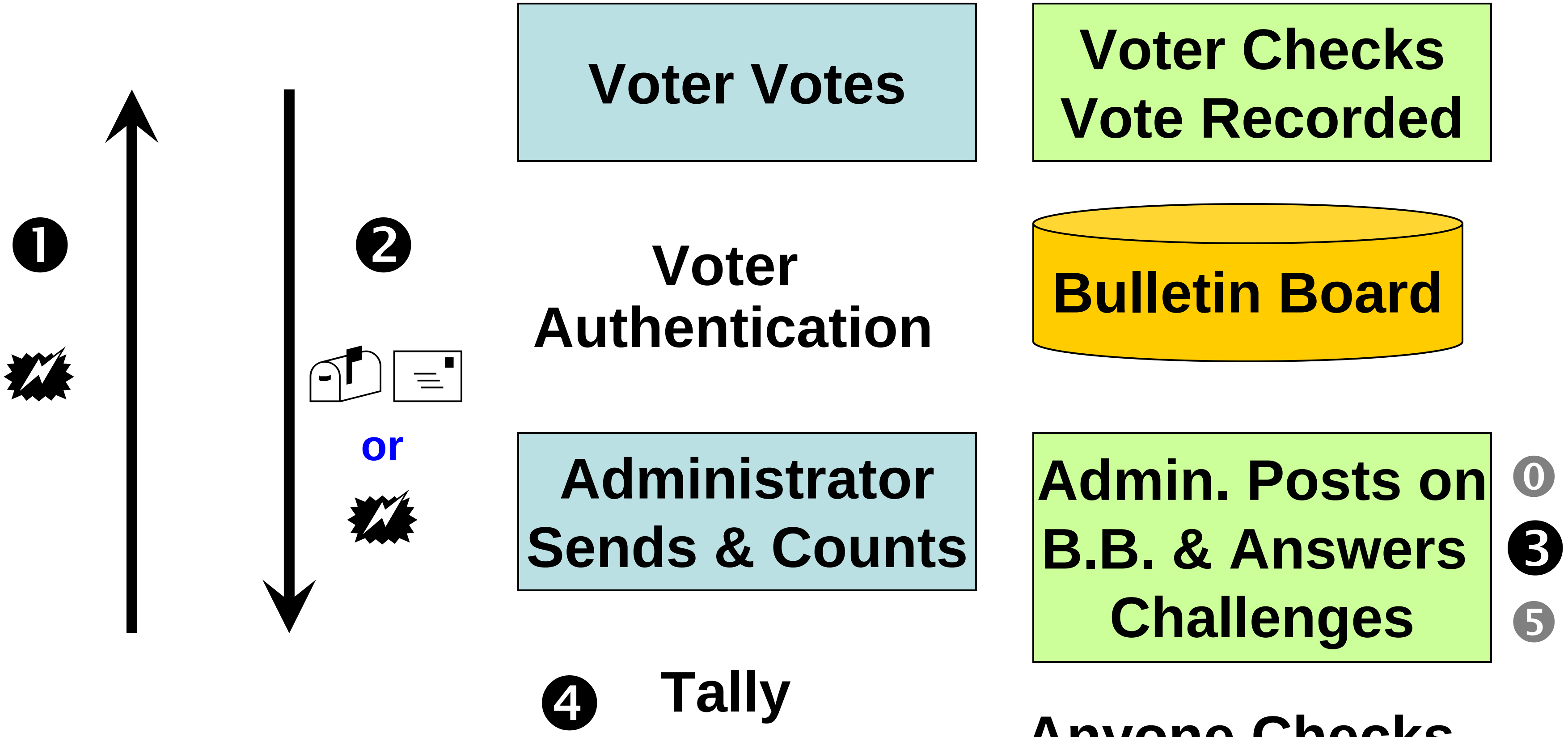
Voter Authentication

Administrator Sends & Counts

Tally

Bulletin Board

# Tallied as Cast Verification



❶

❷

or

Voter Votes

Voter Checks
Vote Recorded

Voter
Authentication

Bulletin Board

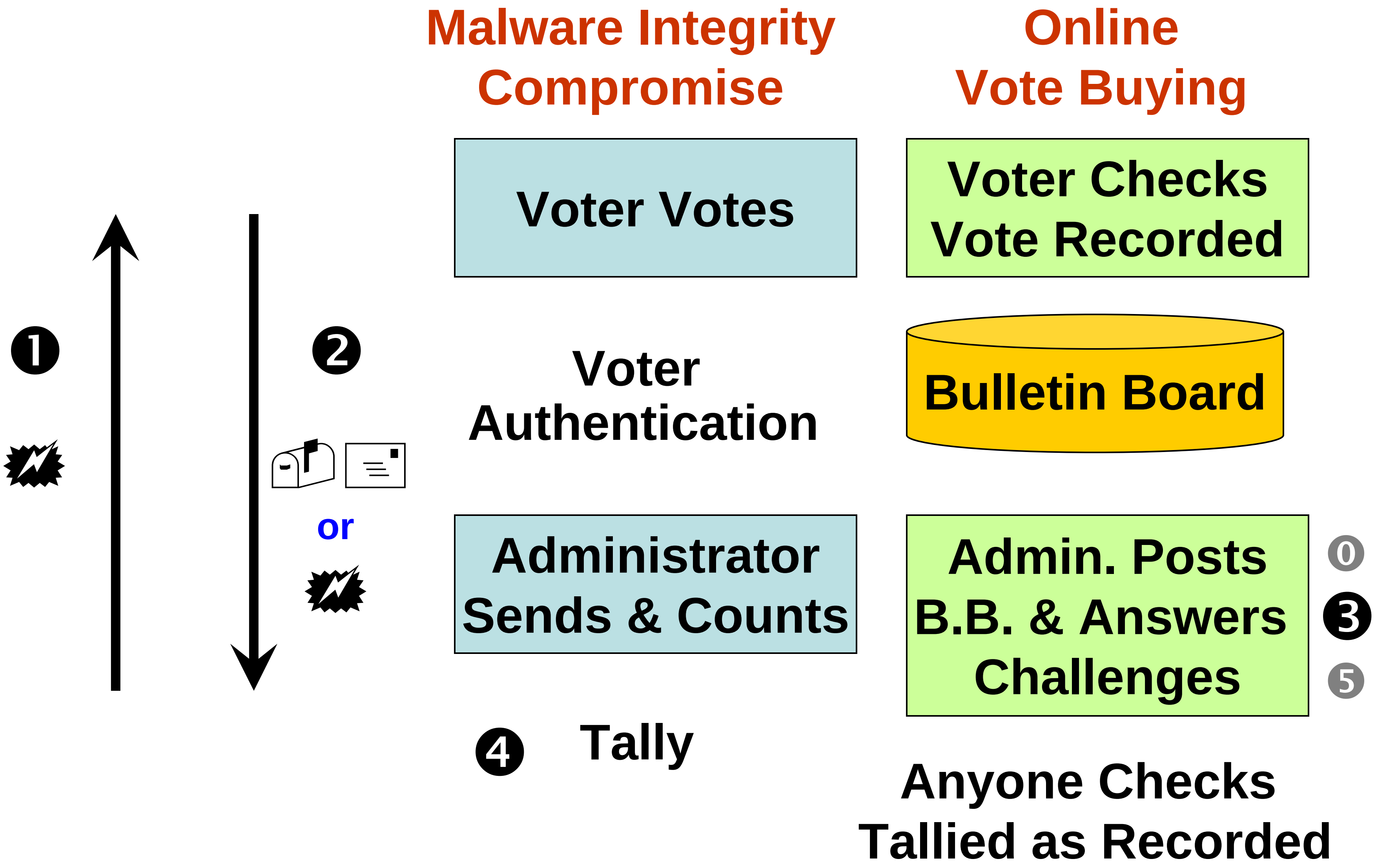
Administrator
Sends & Counts

Admin. Posts on
B.B. & Answers
Challenges

⓿
❸
❺

❹ Tally

Anyone Checks
Tallied as Recorded



Malware Integrity Compromise

Online Vote Buying

❶

❷

or

Voter Votes

Voter Checks Vote Recorded

Voter Authentication

Bulletin Board

Administrator Sends & Counts

Admin. Posts B.B. & Answers Challenges

⓿ ❸ ❺

❹ Tally

Anyone Checks Tallied as Recorded

# Malware Resistance (limited)

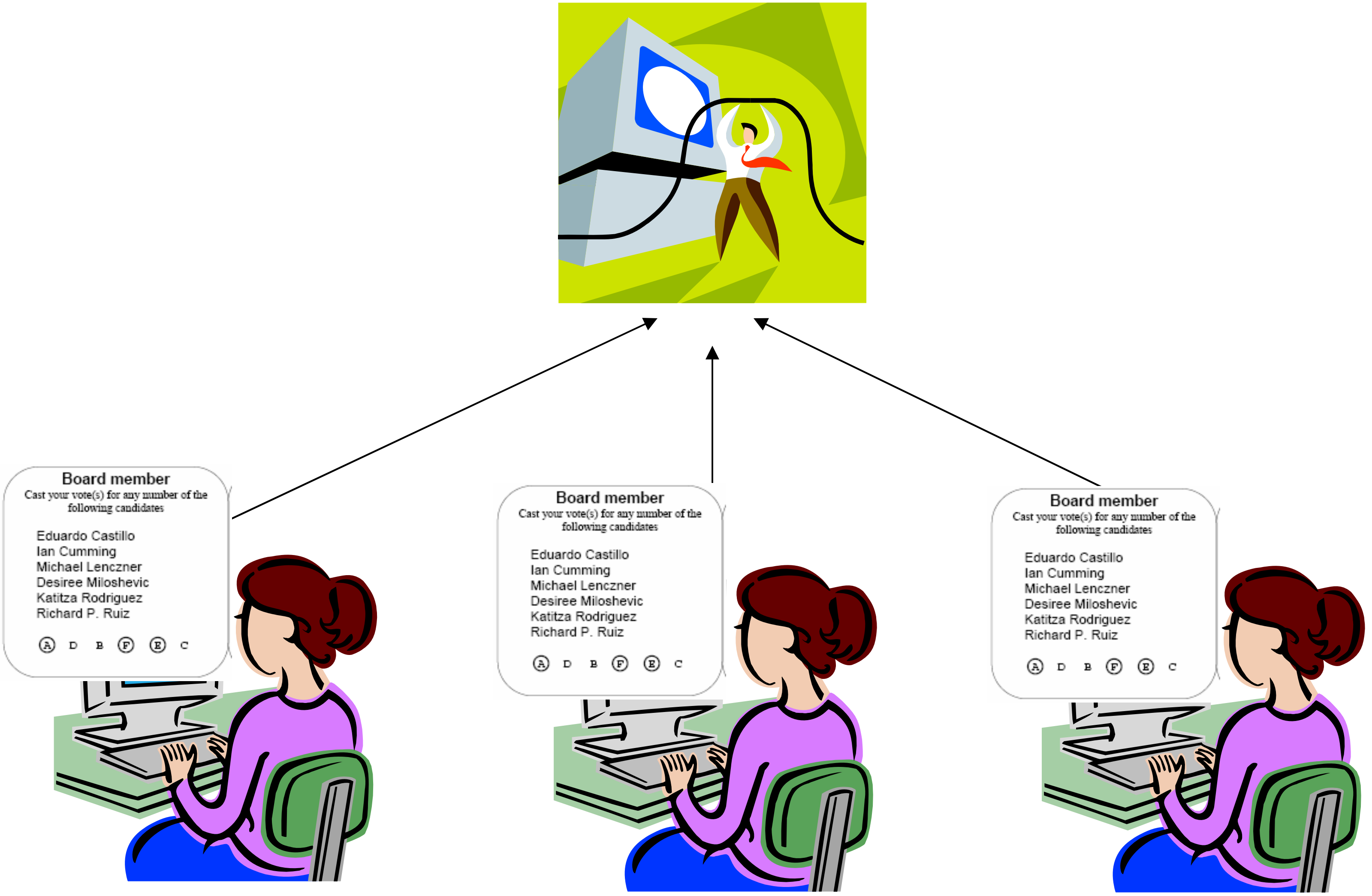
- The voter prints both ballot pages and checks that the vote is correctly encoded – the virus cannot modify the pages once they are printed.
- The voter can check the public bulletin board from multiple computers – presumably not all of which are infected with the same virus.
- If the ballot page posted is not the same as that retained, the voter can request and vote another ballot (blame cannot be assigned)

# Vote Selling Resistance (limited)

- Once the voter decides on the page to send in, the voter can request that a decoy ballot be sent (with matching serial number).
- One page of the decoy ballot is identical to the page the voter already decided to send.
- The other page of the decoy ballot can be created for the voter such that once the voter sends the page originally decided on, the posted page and decoy pages imply that the vote buyer's preferences were voted.

# Voter Experience

# Malware Resistance (limited)



Board member

Cast your vote(s) for any number of the following candidates

Eduardo Castillo
Ian Cumming
Michael Lenczner
Desiree Miloshevic
Katitza Rodriguez
Richard P. Ruiz

Ⓐ D B Ⓕ Ⓔ C

Board member

Cast your vote(s) for any number of the following candidates

Eduardo Castillo
Ian Cumming
Michael Lenczner
Desiree Miloshevic
Katitza Rodriguez
Richard P. Ruiz

Ⓐ D B Ⓕ Ⓔ C

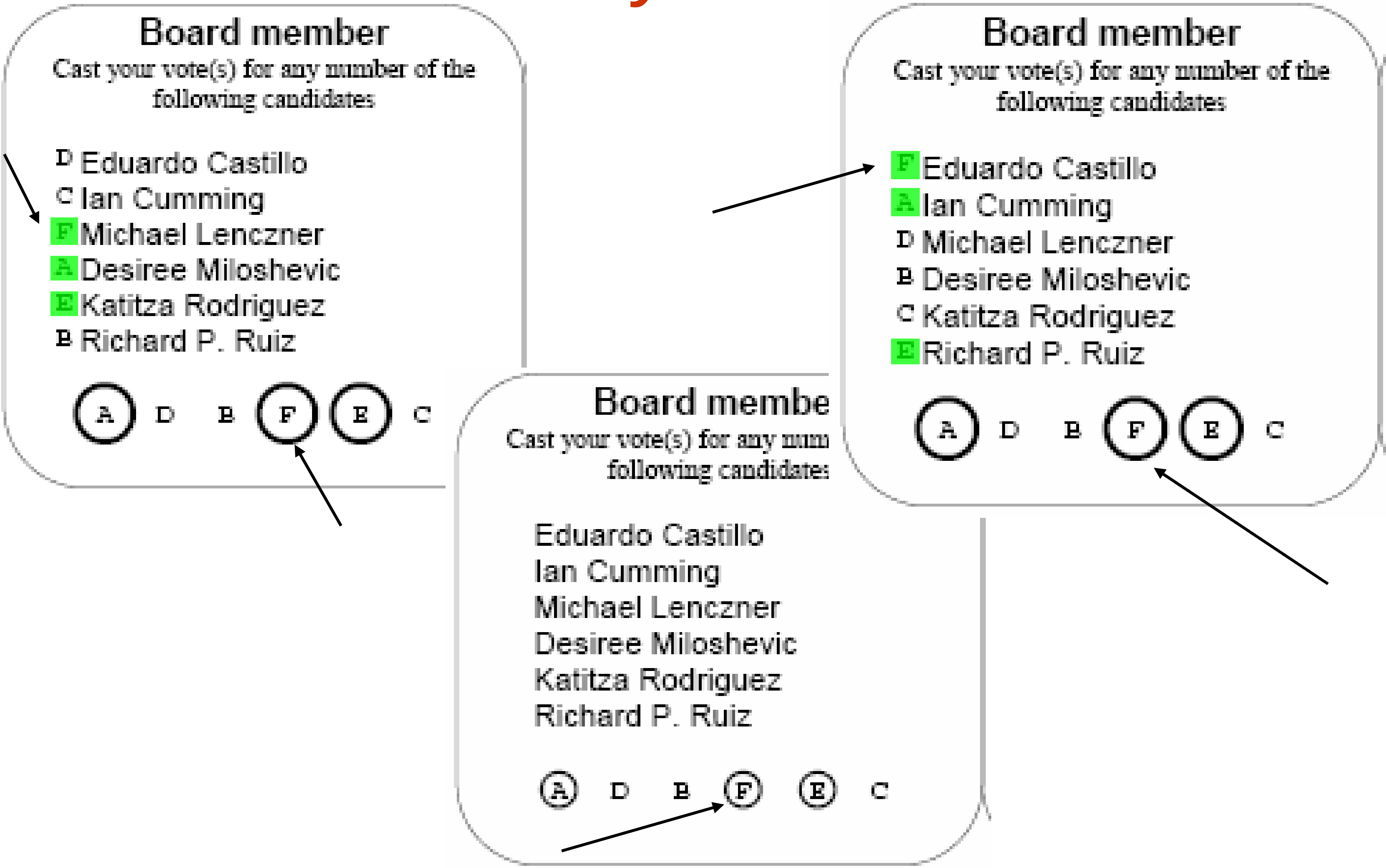
Board member

Cast your vote(s) for any number of the following candidates

Eduardo Castillo
Ian Cumming
Michael Lenczner
Desiree Miloshevic
Katitza Rodriguez
Richard P. Ruiz

Ⓐ D B Ⓕ Ⓔ C

# Decoy Ballots



Board member

Cast your vote(s) for any number of the following candidates

D Eduardo Castillo
C Ian Cumming
🟩F Michael Lenczner
🟩A Desiree Miloshevic
🟩E Katitza Rodriguez
B Richard P. Ruiz

[✓ A] D B [✓ F] [✓ E] C

Board member

Cast your vote(s) for any number of the following candidates

🟩F Eduardo Castillo
🟩A Ian Cumming
D Michael Lenczner
B Desiree Miloshevic
C Katitza Rodriguez
🟩E Richard P. Ruiz

[✓ A] D B [✓ F] [✓ E] C

Board membe

Cast your vote(s) for any num following candidates

Eduardo Castillo
Ian Cumming
Michael Lenczner
Desiree Miloshevic
Katitza Rodriguez
Richard P. Ruiz

[✓ A] D B [✓ F] [✓ E] C

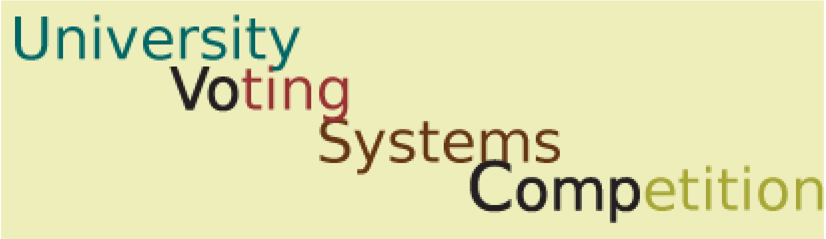
# Software Steps

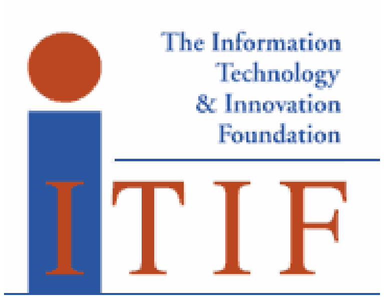
- Import PDF ballot and export the unique links
- Publish commitments
- Open commitments (stock quote challenges)
- Serve up the ballots (based on links)
- Post the receipts
- Post the results
- Post audit data (stock quote challenges)

# The Software

- All the code is open source – all the libraries it uses are open source
- Three versions were released during the past 22 months
- Core is in Java – buildable with ANT and runnable online with JNLP (the web pages are in PhP)

# Several Elections with the Back-End





# 2008 CPSR Board of Directors

CPSR Computer Professionals For Social Responsibility

# Requirements for voters

- Email
- Browser (any)
- Adobe Reader 5.0 or higher
  - with JavaScript enabled (the default)
  - Works on : Windows, Macintosh, Linux, Solaris, HP-UX, AIX.
- Printer
- Optional: Fax

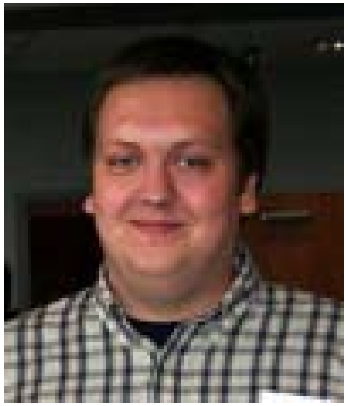
# Performance

- 10.000 Ballots cast,11 contests, 38 candidates
- On an Intel Core Duo 1.73GHz, 1Gb Ram
  - Overall total for the election administrator: 20 seconds
  - Auditing the results in 2 seconds

# The PunchScan team
# *www.punchscan.org*

David Chaum

Rick Carback



UMBC
AN HONORS UNIVERSITY IN MARYLAND

Jeremy Clark

UNIVERSITY OF
Waterloo

Aleks Essex

uOttawa
L'Université canadienne
Canada's university

Stefan Popoveniuc

THE GEORGE WASHINGTON UNIVERSITY