Technical Overview

David Chaum

WOTE

Outline of Presentation

- Concept

  (for basic SureVote version)
- User Interface Options

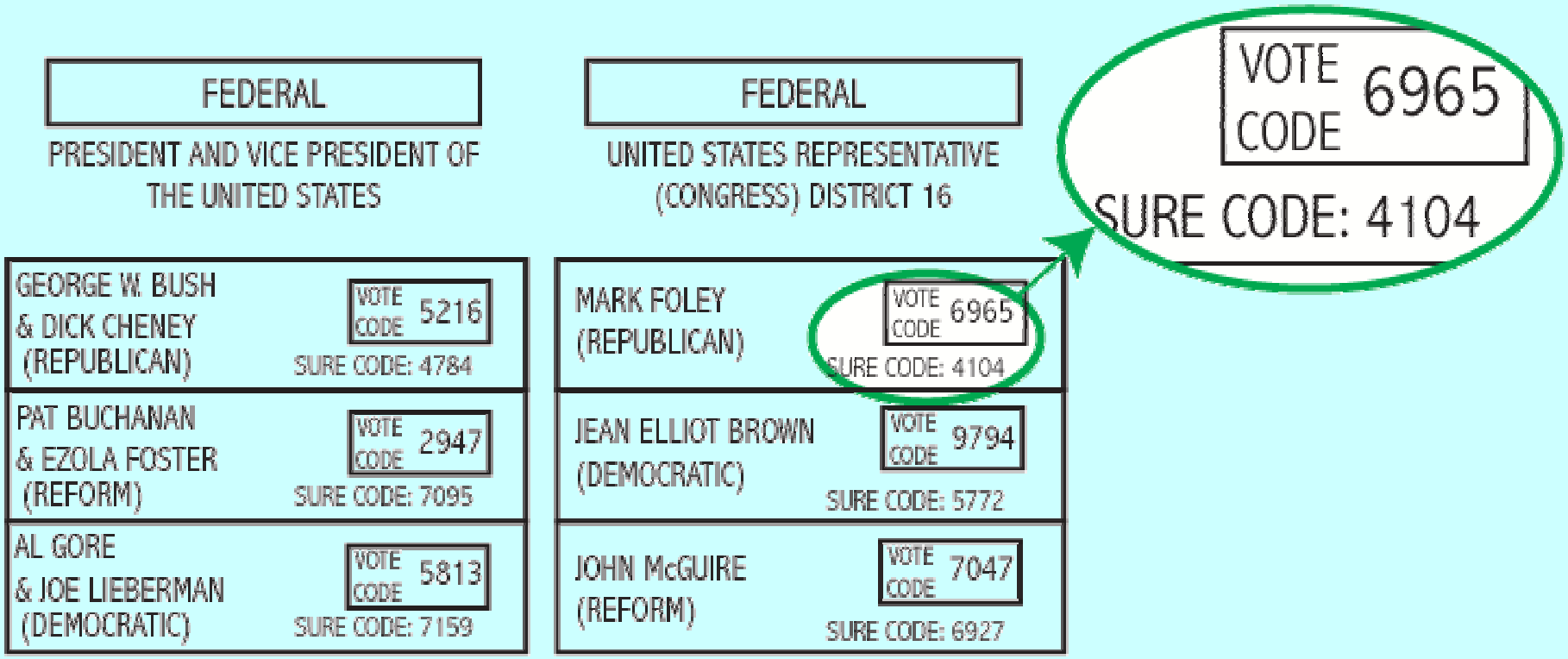
  (and their implications)
- Process Flow Detail

  (multi-server case)
- Variations & Extensions

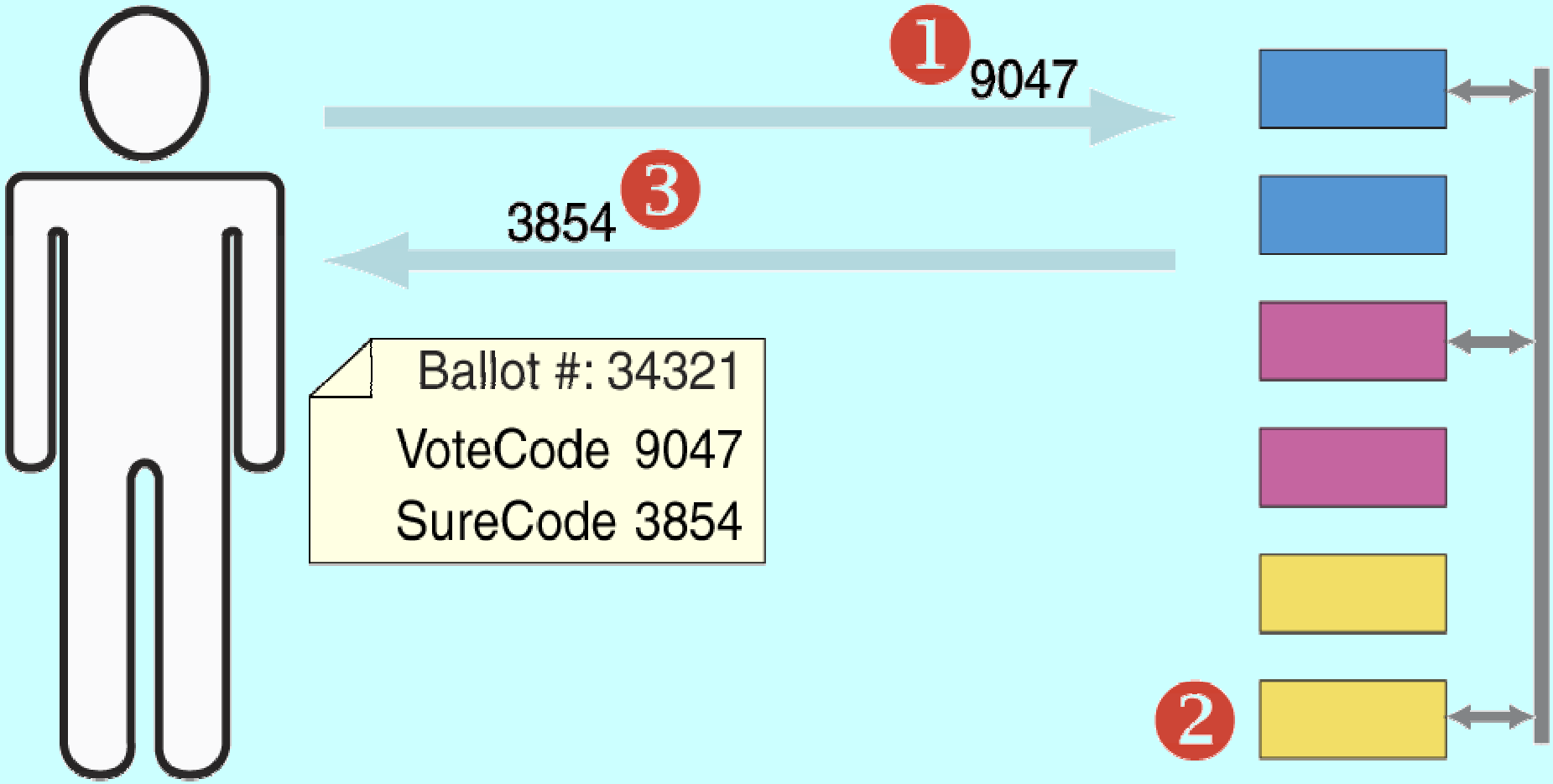
  (offline, non-geographic, exit devices, control votes, ballot-style security, single-server, etc.)

Simple SureVote Ballot

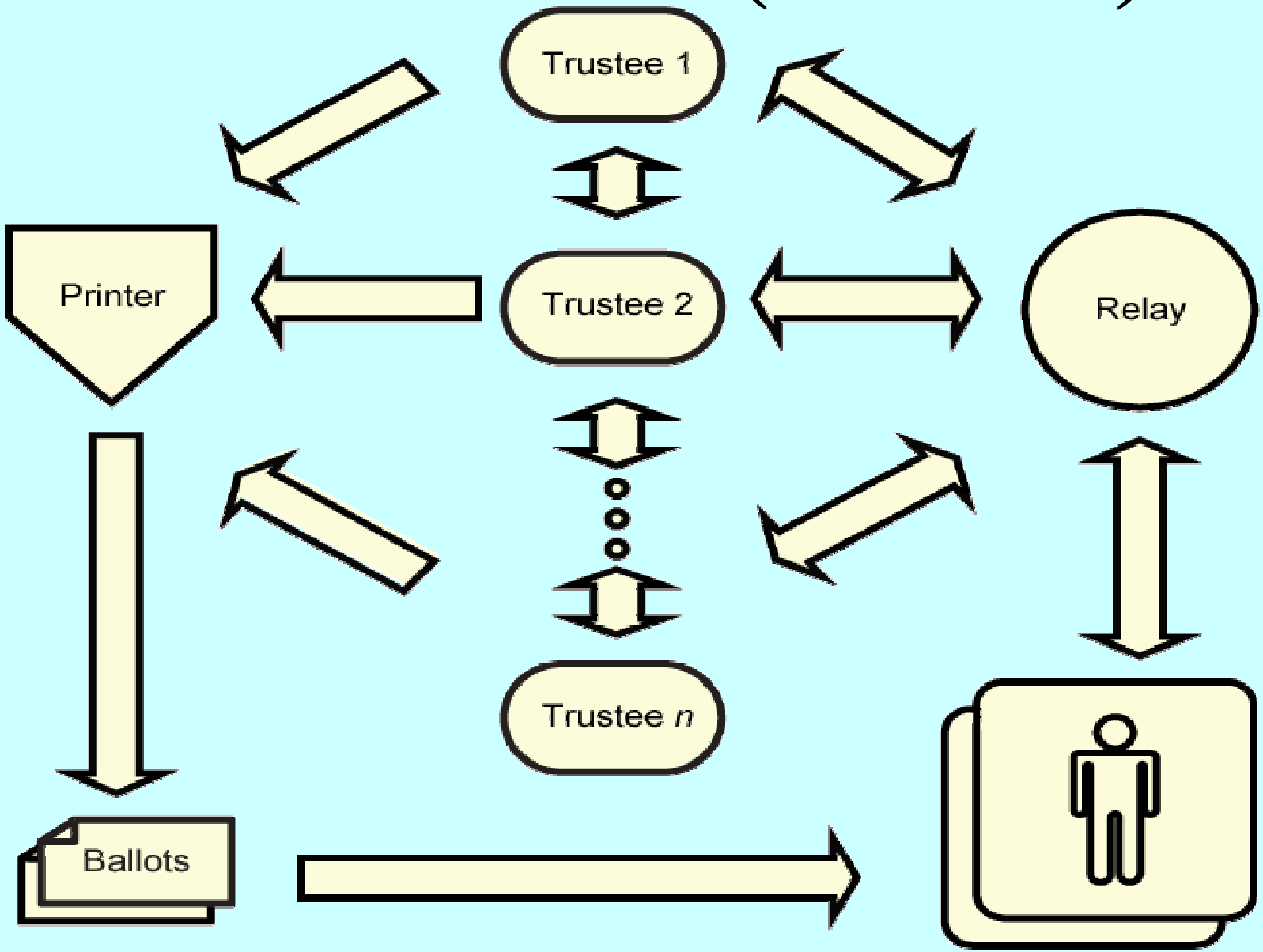
Ballot #: **52234**



Voting Process (overview)



Overall Process (overview)



What are the main reasons SureVote is so interesting?

- **No machines to trust at precinct!**
  - **Much higher integrity**
  - **Much lower cost**
- **Voter authenticates system and choice!**
  - **More accuracy**
  - **Higher voter confidence**
- **Integrated attendance and remote**
- **Non-Geographic and permissive voting**

User Interface Examples

- ***Web browser***

  (which contests revealed UI)
- ***Barcode***
- ***Telephone***

  (number of contests revealed to UI)
- ***Human Intermediary***
- ***Touchscreen***

  (choices must be revealed to UI)

Web

Ballot #:78694

Vote Code: 2304 Sure Code: 1698	SUBMIT
President and Vice President of the United States	United States Representative (Congress) District #16
George W. Bush & Dick Cheney (Republican)	Mark Foley (Republican)
Pat Buchanan & Ezola Foster (Reform)	Jean Elliot Brown (Democratic)
Al Gore & Joe Liberman (Democratic)	John McGuire (Reform)

Barcode

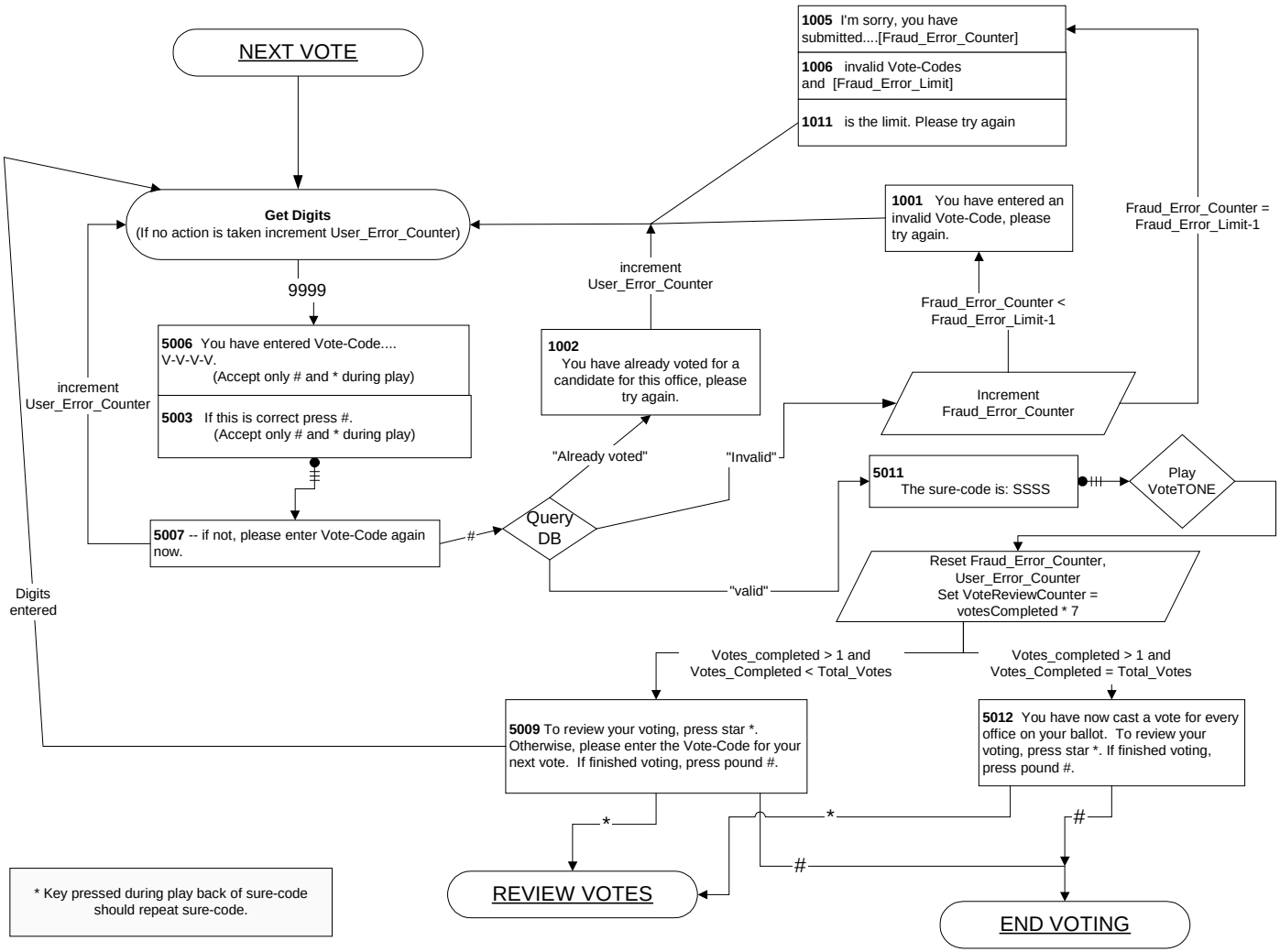
Ballot #: **78694**

FEDERAL

PRESIDENT AND VICE PRESIDENT OF THE UNITED STATES

GEORGE W. BUSH & DICK CHENEY (REPUBLICAN)	VOTE CODE 2304	SURE CODE: 1698
PAT BUCHANAN & EZOLA FOSTER (REFORM)	VOTE CODE 7406	SURE CODE: 2425
AL GORE & JOE LIEBERMAN (DEMOCRATIC)	VOTE CODE 8991	SURE CODE: 8753

Telephone (Remote or Attendance Voting)



Human Intermediary

- Unlike “Assisted Voting”
  - No integrity/influencing vulnerability
  - No privacy exposure
- Expands access
  - Beyond usual disability definition
  - Also includes illiterates

Touchscreen

President and Vice President of the United States
George W. Bush & Dick Cheney (Republican)
Pat Buchanan & Ezola Foster (Reform)
Al Gore & Joe Lieberman (Democratic)

Process Overview

1. **Ballot preparation—for all ballots**
   - ***Committing, printing, checking***
2. **Voting—for each ballot** [not detailed]
   - ***Exchanging SureCodes for VoteCodes***
3. **Tabulating—for all voted ballots**
   - ***Two passes through trustees, checking***

1. Ballot Preparation

i. Commitments to codes are published

- Pins created by each trustee
- Shift amounts created by each trustee
- Trustees each publish commits to all values

ii. Printing of paper ballots

- Trustees furnish values to printer
- Printer combines (addition modulo max value)
- Printer prints codes “rotated” by shift amount

iii. Checking ballots & commitments

- “Auditors” choose ballots to open at random
- Trustees open commitments for opened ballots
- Auditors check consistency

3. Tabulating

i. Computing and publishing proofs

- Entire batch passes through trustees twice
- *First phase:* trustees add in two exponents, one for shift (different per item) one for encryption (same for all items) [no mixing]
- *Second phase:* trustees remove encryption exponent and output batch in permuted order [mixing]

ii. Checking proofs

- Verify that the ballot images output correspond to the originally committed ballots and committed votes

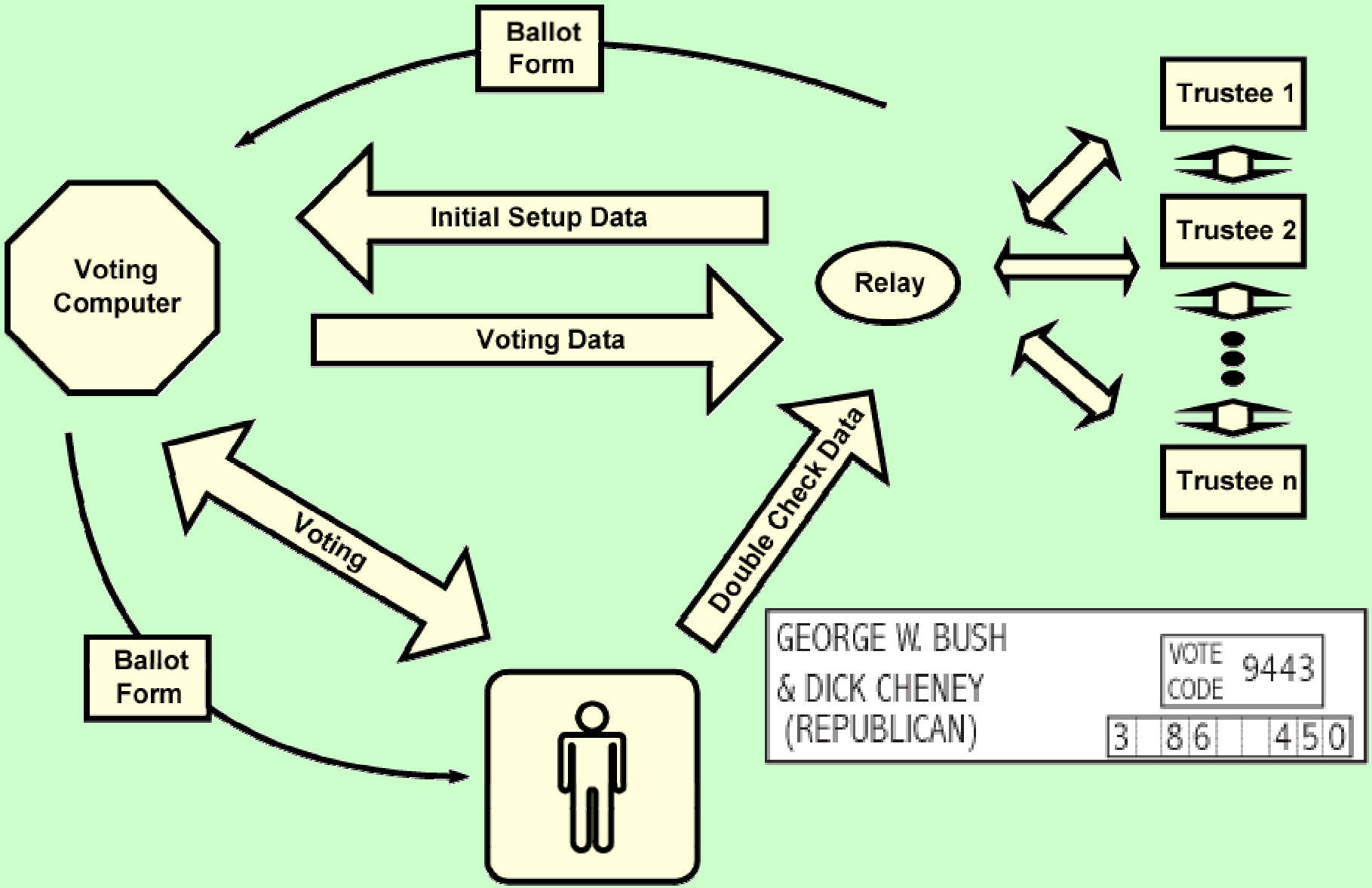
Variations & Extensions

- ***re-tally***
- ***Online/offline attendance voting***
- ***Non-Geographic***
- ***Write-in and type-in***
- ***Scratch-off printing***
  - ***Indelible ballots***
  - ***Self-shredding ballots***
- ***Control votes & exit devices***
- ***Single & multiple server applications***

Re-tally

- ***Example uses:***
  - ***Permissive registration/contested ballot***
  - ***Court ordered inclusion/exclusion (formerly required spoiling precinct)***

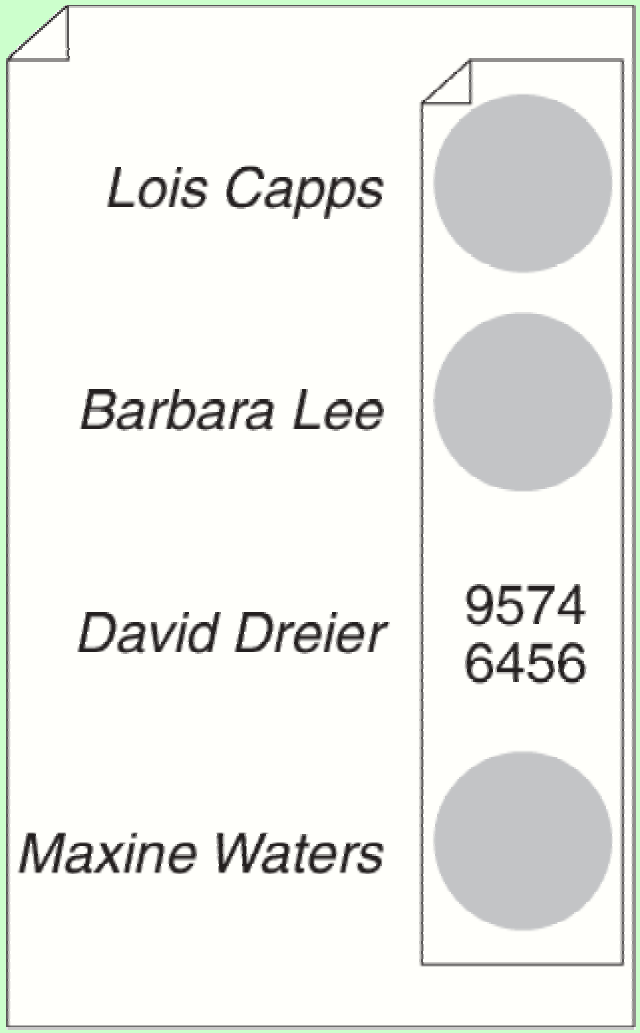
Online/Offline



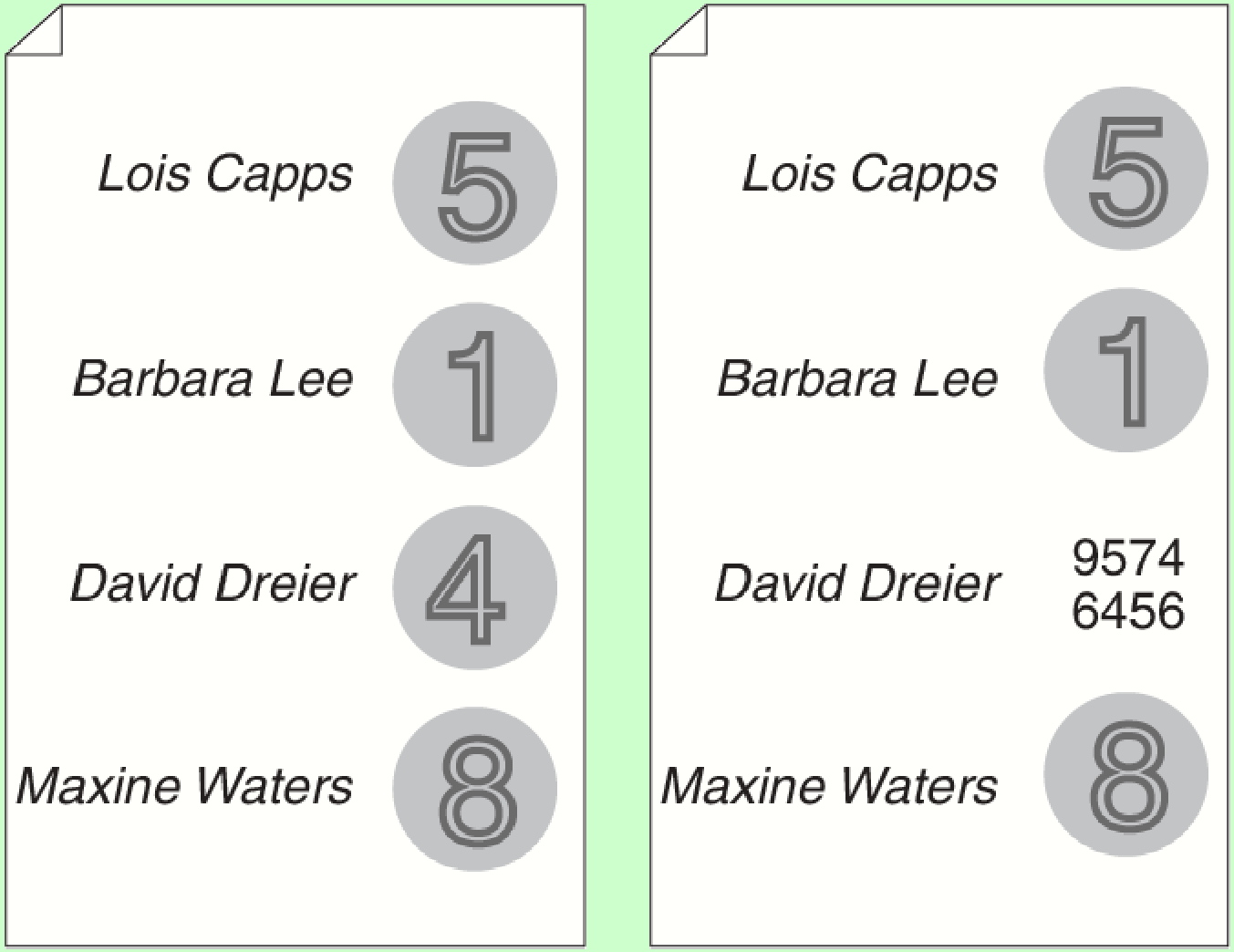
Non-Geographic

- ***Example uses of "one big precinct"***
  - ***Early voting (e.g., countywide)***
  - ***Absentee ballot***
  - ***Attendance at non-home precinct***

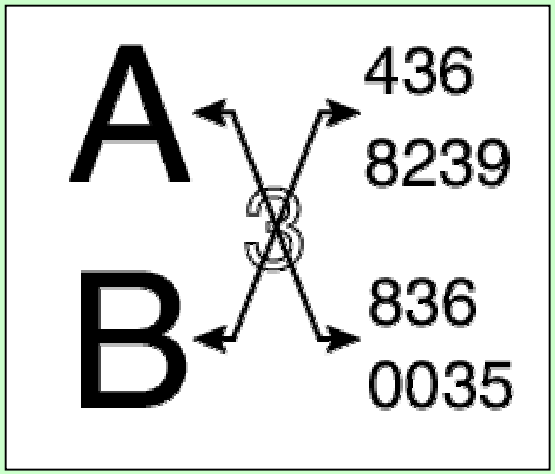
Demand-Printed Ballot

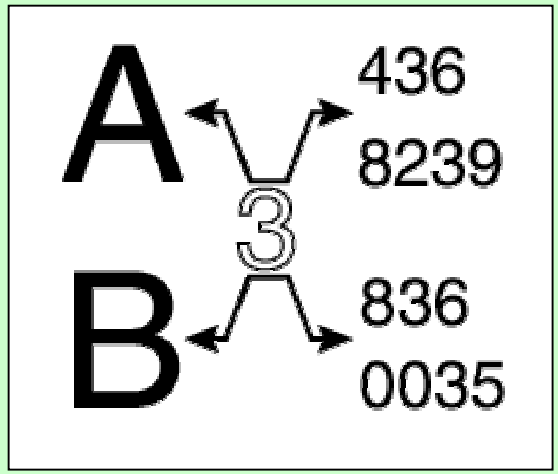


Indelible Ballots



Self-Shredding Ballots



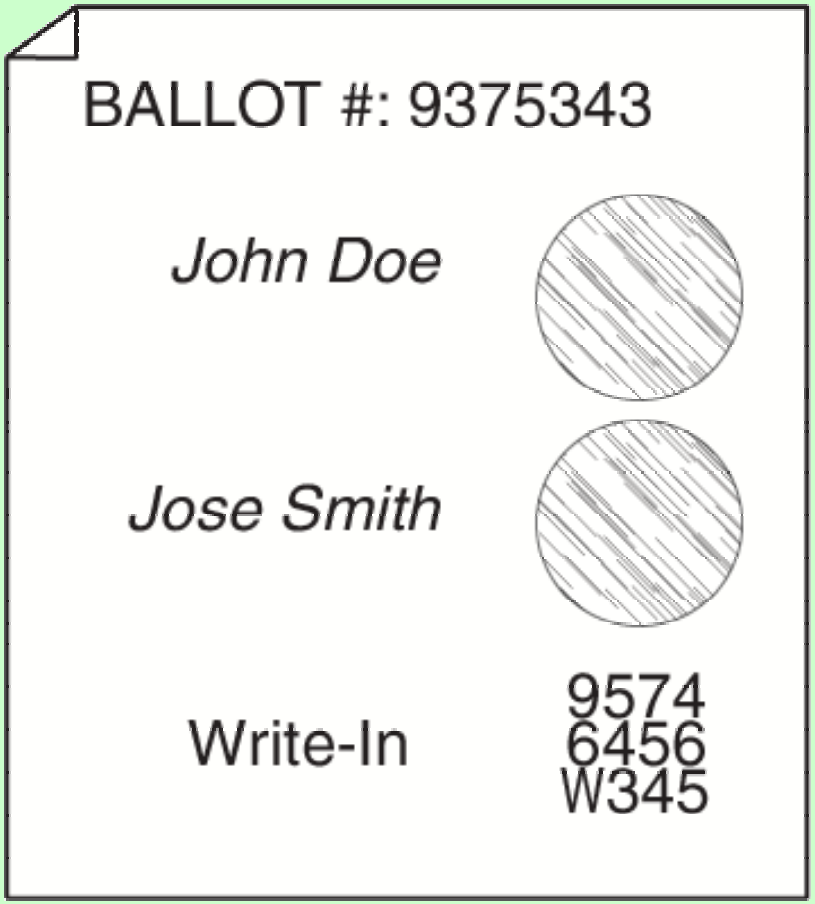


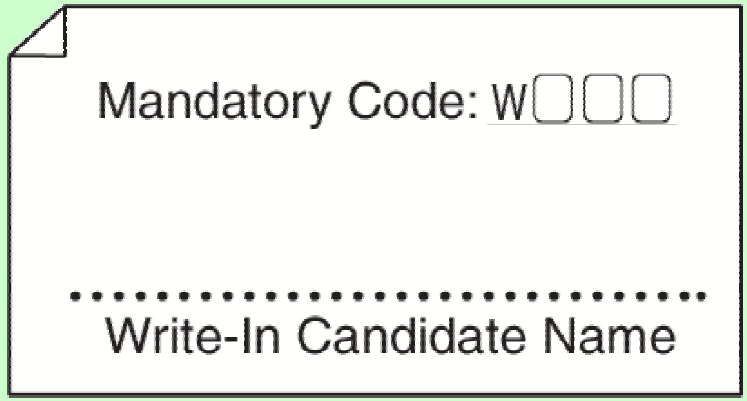
Once arrows are scratched off to reveal numbers, choice is permanently destroyed.

Type-in

7435	6583	9474	3608	4765	3235	6863
8763	5643	7548	7805	5427	0765	4534
6355	0654	0966	8653	2595	9643	8768
8765	4673	4367	6658	3409	9054	6435
9574	5645	5465	4565	3443	5645	4534
6456	5465	4565	5465	6544	6544	3454
5445	4876	5435	1018	7654	3246	4324
9573	7653	3486	0187	0865	3454	3423

Write-In


BALLOT #: 9375343
John Doe
Jose Smith
Write-In
9574
6456
W345


Mandatory Code: W
Write-In Candidate Name

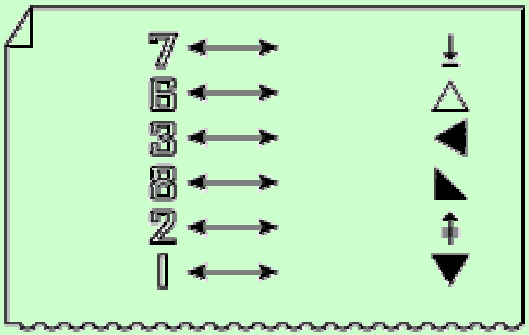
Ballot-Style Security

- ***You can take your ballot home!***
  - ***Shredding also possible***

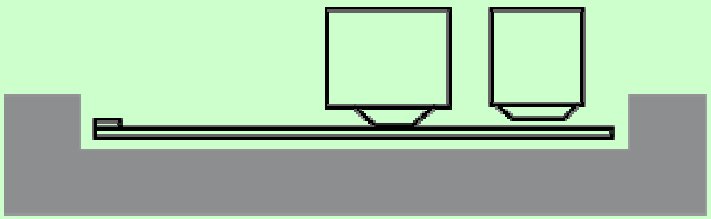
Cast/Spoilt Control Votes

- ***Control votes can lock a ballot***
- ***Control vote can make a ballot spoilt***

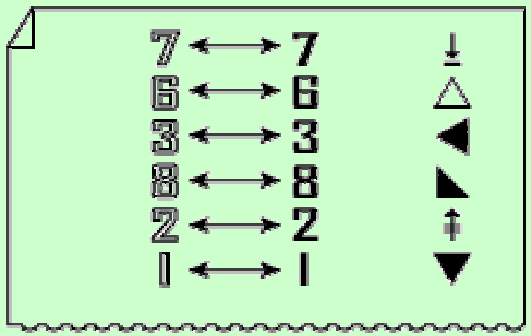
Counterfoil Printer
Example Exit Device



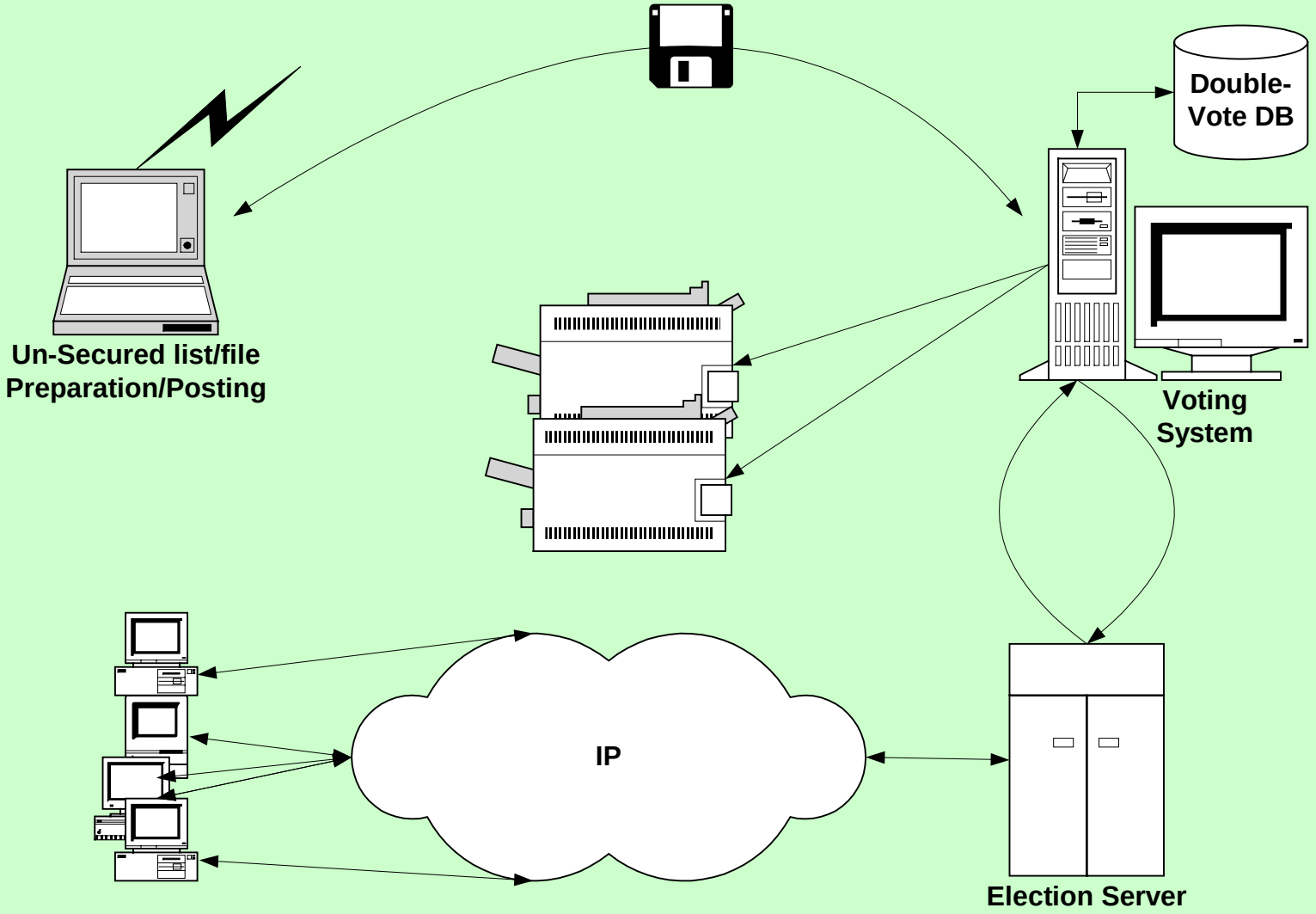
Before



After



Single-Server System



Multiple-Server Configuration Options

- ***Each political party has server***
  - ***e.g., Democrats, Republicans, etc.***
- ***Government hierarchy of servers***
  - ***County has its own server(s)***
  - ***State & Federal can too***
- ***Monitoring countries have servers***
  - ***Critical emerging country elections***

Conclusion

- **Higher integrity & confidence**
- **Lower cost**
- **Robust**
- **Attendance & Remote in real-time**
- **Non-Geographic**
- **Permissive re-tally**
- **Multi-server**