2550 Intro to cybersecurity

L16: Voting

abhi shelat/Ran Cohen

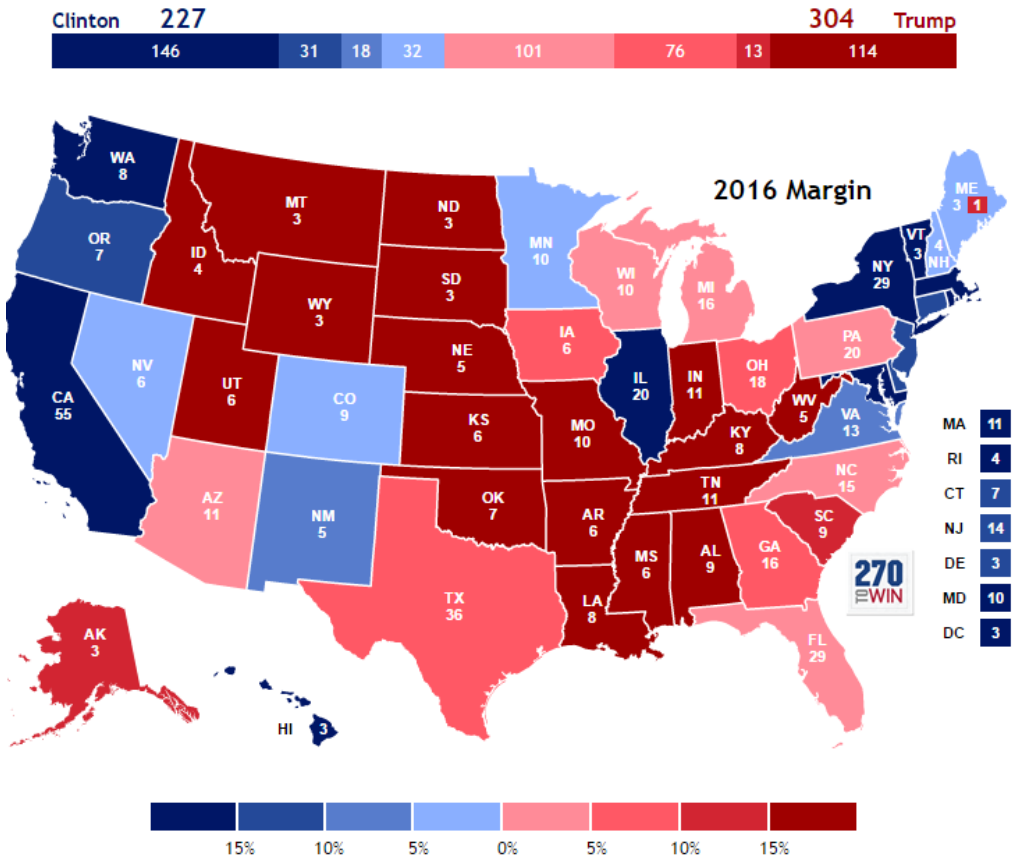
Thanks to Alon Rosen (IDC) and Ron Rivest (MIT) for sharing slides

Flashback: U.S. 2016 Presidential Election

How Close was the Election?

- Clinton received nearly 3 million more votes
- Trump won the Electoral College
- There were 137 million votes
- How many votes would need to change for a tie?
- 30,765 (0.02%)

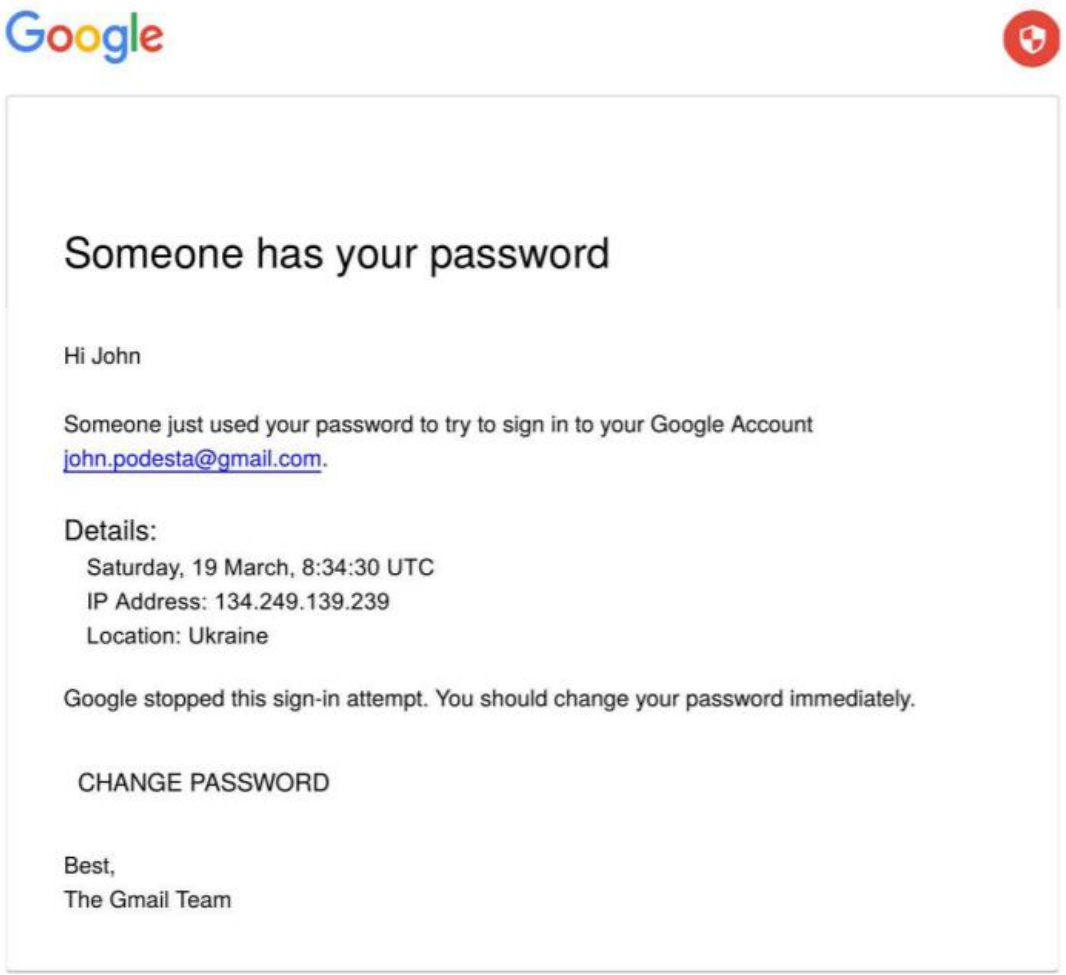
MI	5,352	(0.1%)	16EV
PA	22,146	(0.4%)	20EV
ND-2	3,267	(1.2%)	1EV
WI	11,374	(0.4%)	10EV
FL	56,455	(0.6%)	29EV
AZ	45,617	(1.8%)	11EV
NC	86,657	(1.8%)	15EV



https://www.270towin.com/2016_Election

2016 Russian Interference

- Targeted political leaks
  (John Podesta spear phishing)



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

2016 Russian Interference

- Targeted political leaks
  (John Podesta spear phishing)
- Trolling/fake news

The New York Times

The Fake Americans Russia Created to Influence the Election

https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

2016 Russian Interference

- Targeted political leaks (John Podesta spear phishing)
- Trolling/fake news
- Attacking election infrastructure
  - Multiple states infiltrated (SQL injection, etc.)
  - Ability to change/destroy registration data

Sections ☰

The Washington Post
Democracy Dies in Darkness

What we know about the 21 states targeted by Russian hackers

https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers

2016 Russian Interference

- Targeted political leaks (John Podesta spear phishing)
- Trolling/fake news
- Attacking election infrastructure
  - Multiple states infiltrated (SQL injection, etc.)
  - Ability to change/destroy registration data

The New York Times

Russia Targeted Election Systems in All 50 States, Report Finds

A voter casting his ballot in the midterm elections last year in Medina, N.D. Hilary Swift for The New York Times

By David E. Sanger and Catie Edmondson

July 25, 2019

714

https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

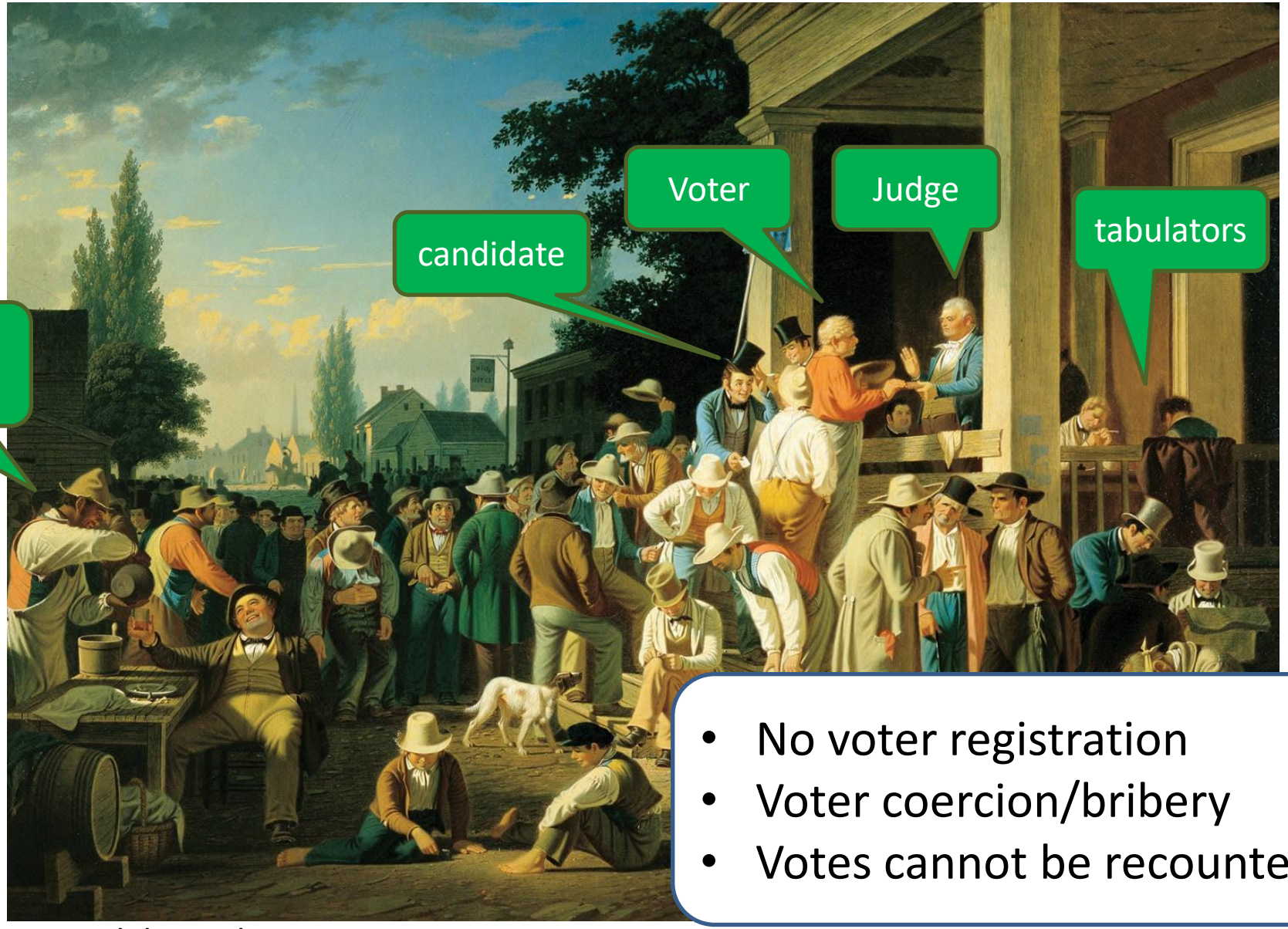
Outline

- History of U.S. voting
- Guidelines for secure voting
- Crypto-based voting

Paperless voting, 1846

The County Election, George Caleb Bingham, 1852

Paperless voting, 1846



- No voter registration
- Voter coercion/bribery
- Votes cannot be recounted

The County Election, George Caleb Bingham, 1852

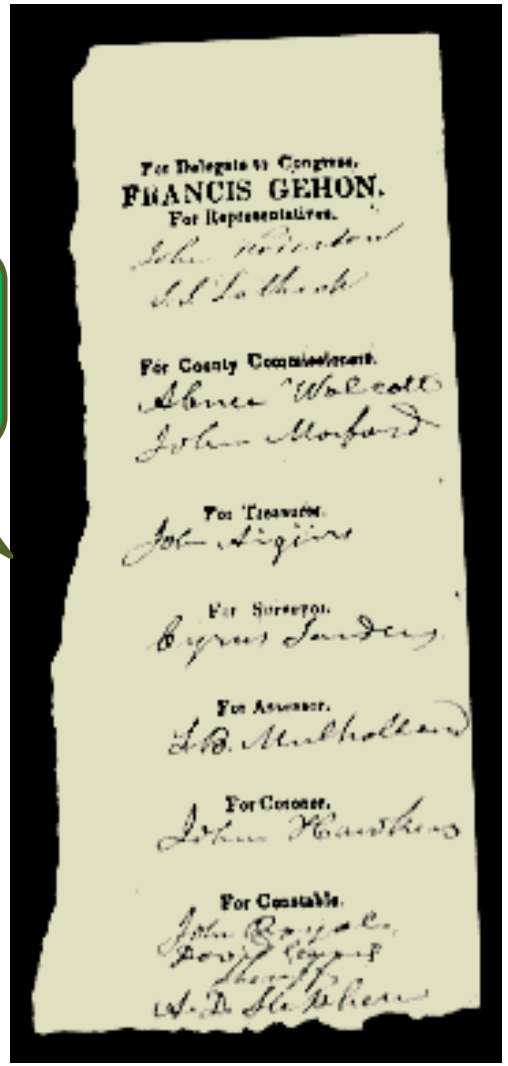
Paperless voting

"The Election—At the Polls," W.J.H., 1857. Library of Congress

Paper Ballots

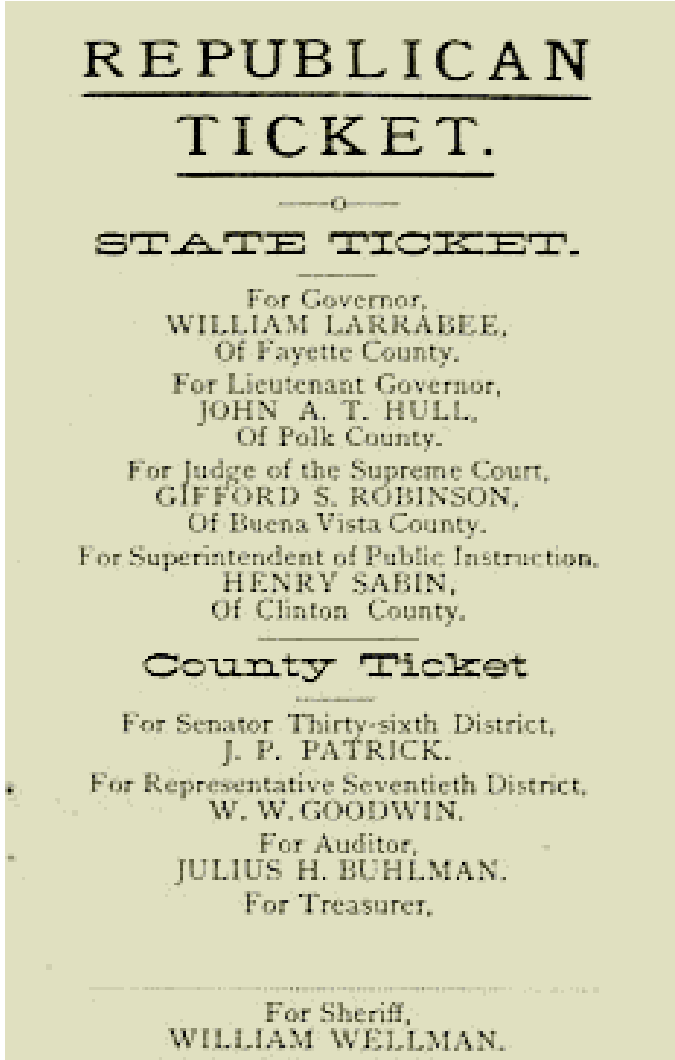
Ballot printed as an advertisement in a newspaper

Each person brings its ballot from home



IOWA, 1839

https://homepage.cs.uiowa.edu/~jones/voting/pictures/



REPUBLICAN TICKET.

STATE TICKET.

For Governor,
WILLIAM LARRABEE,
Of Fayette County.

For Lieutenant Governor,
JOHN A. T. HULL,
Of Polk County.

For Judge of the Supreme Court,
GIFFORD S. ROBINSON,
Of Buena Vista County.

For Superintendent of Public Instruction,
HENRY SABIN,
Of Clinton County.

County Ticket

For Senator Thirty-sixth District,
J. P. PATRICK.

For Representative Seventieth District,
W. W. GOODWIN.

For Auditor,
JULIUS H. BUHLMAN.

For Treasurer,

For Sheriff,
WILLIAM WELLMAN.

IOWA, 1888

No room to strike out and replace

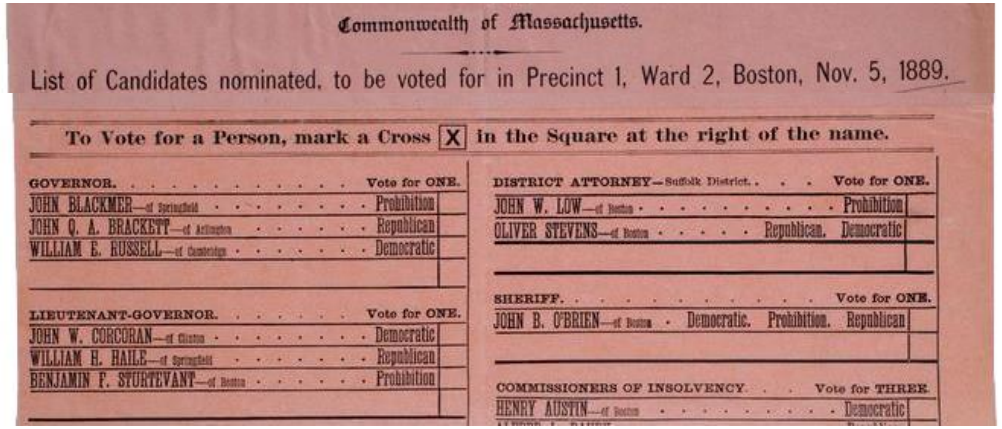
Each party printed its ballots in a distinct newspaper (no secrecy)

Requirements from Voting

- Allow each person to vote (just) once
- Accurately count the votes
- Can’t learn how other people voted
- Each voter can verify its vote is counted
- No one can reveal to whom they voted (no vote selling)

The Australian Ballot

- An official ballot being printed at public expense
- The names of the candidates of all parties and all proposals appear,
- Distributed only at the polling place and
- Marked in secret.



Commonwealth of Massachusetts.

List of Candidates nominated, to be voted for in Precinct 1, Ward 2, Boston, Nov. 5, 1889.

To Vote for a Person, mark a Cross [X] in the Square at the right of the name.

GOVERNOR. . . . . Vote for ONE.
JOHN BLACKMER—of Springfield . . . . . Prohibition
JOHN Q. A. BRACKETT—of Arlington . . . . . Republican
WILLIAM E. RUSSELL—of Cambridge . . . . . Democratic

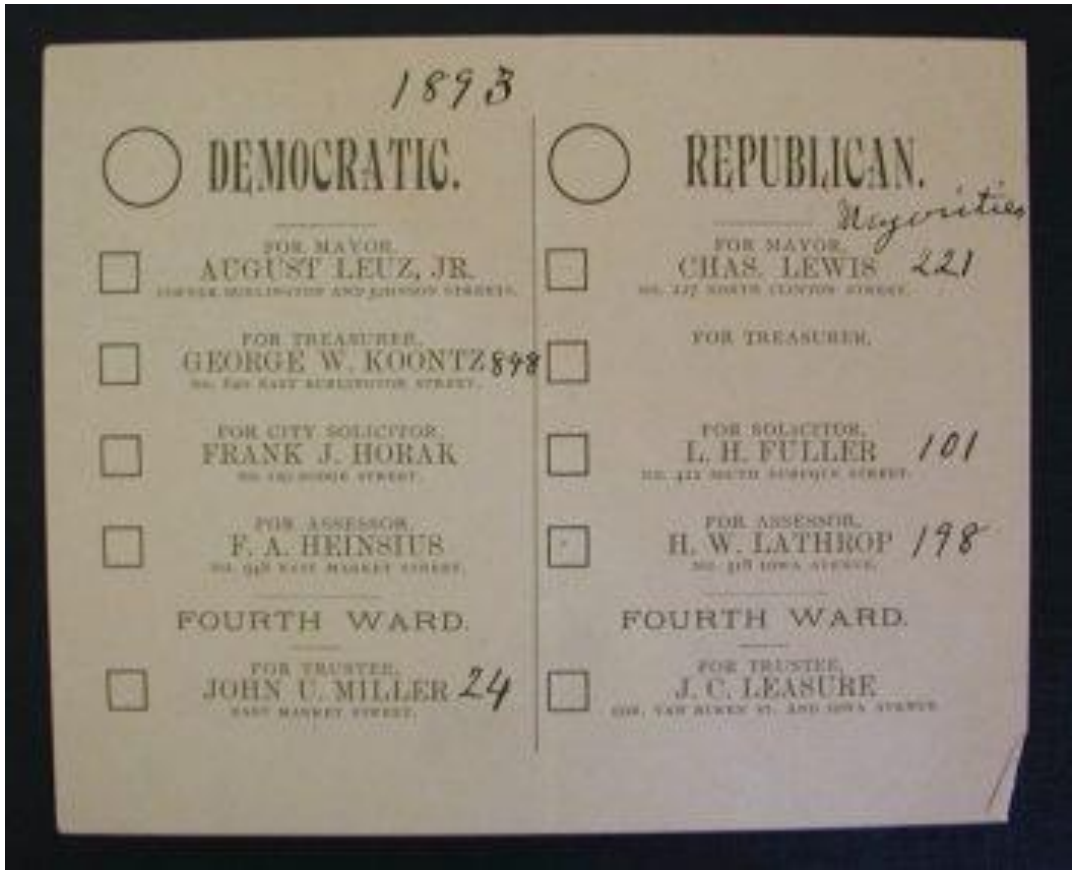
LIEUTENANT-GOVERNOR. . . . . Vote for ONE.
JOHN W. CORCORAN—of Clinton . . . . . Democratic
WILLIAM H. HAILE—of Springfield . . . . . Republican
BENJAMIN F. STURTEVANT—of Boston . . . . . Prohibition

DISTRICT ATTORNEY—Suffolk District. . . . Vote for ONE.
JOHN W. LOW—of Boston . . . . . Prohibition
OLIVER STEVENS—of Boston . . . . . Republican. Democratic

SHERIFF. . . . . Vote for ONE.
JOHN B. O'BRIEN—of Boston . Democratic. Prohibition. Republican

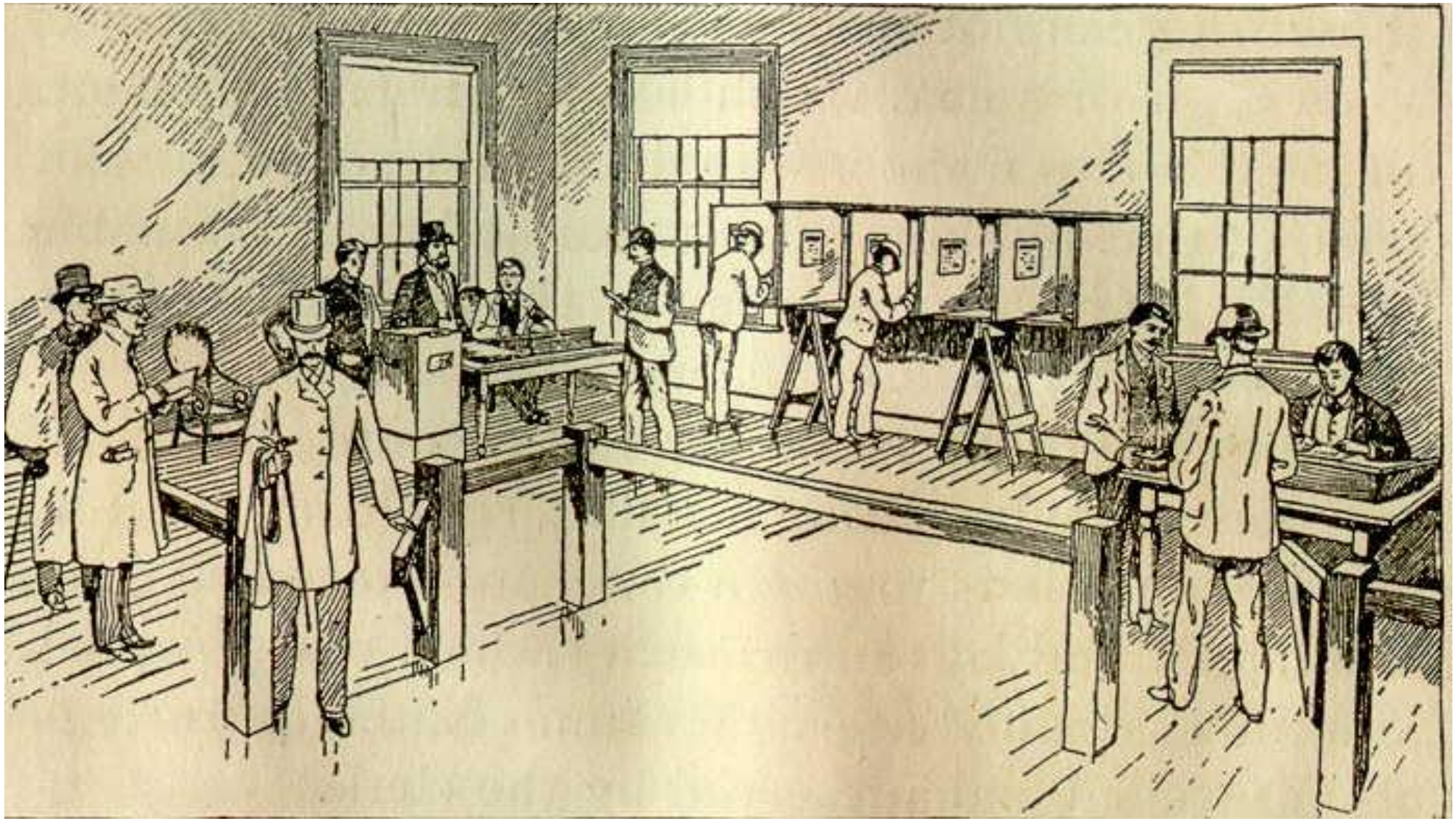
COMMISSIONERS OF INSOLVENCY. . . Vote for THREE.
HENRY AUSTIN—of Boston . . . . . Democratic

https://www.newyorker.com/culture/culture-desk/this-is-what-democracy-looked-like



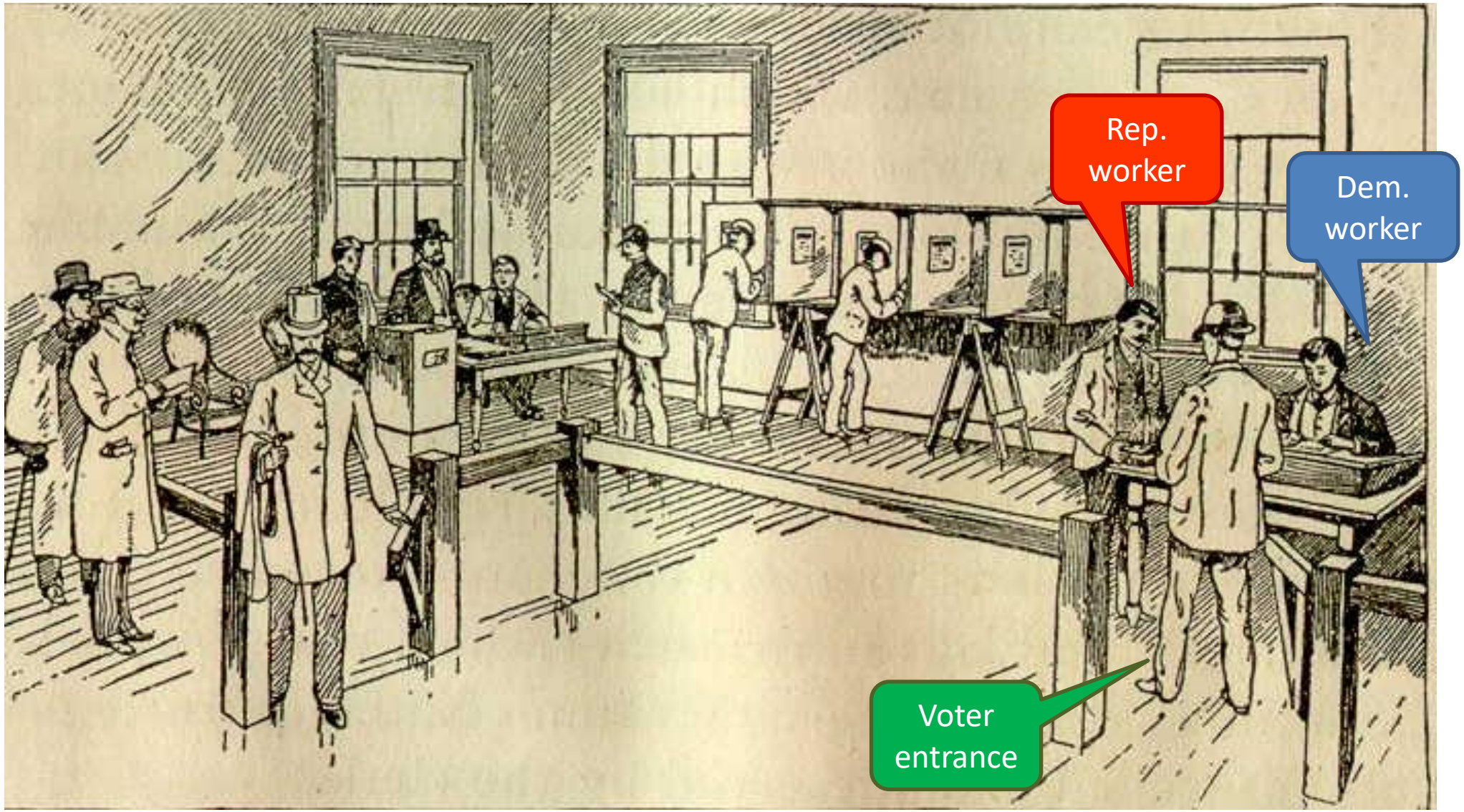
https://homepage.cs.uiowa.edu/~jones/voting/pictures/

Secret Ballots, 1890



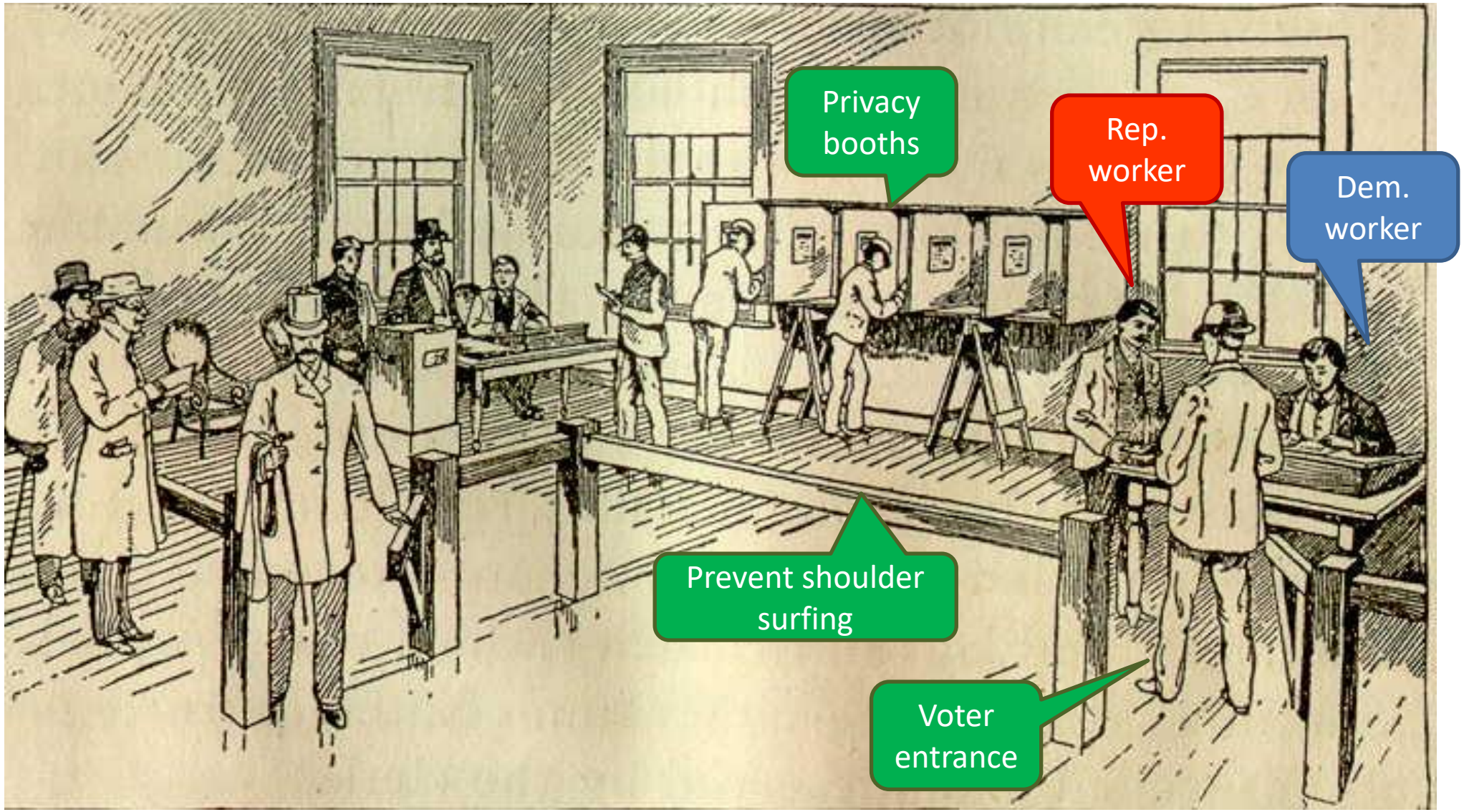
From Elements of Civil Government by Alexander L. Peterman, 1891

Secret Ballots, 1890



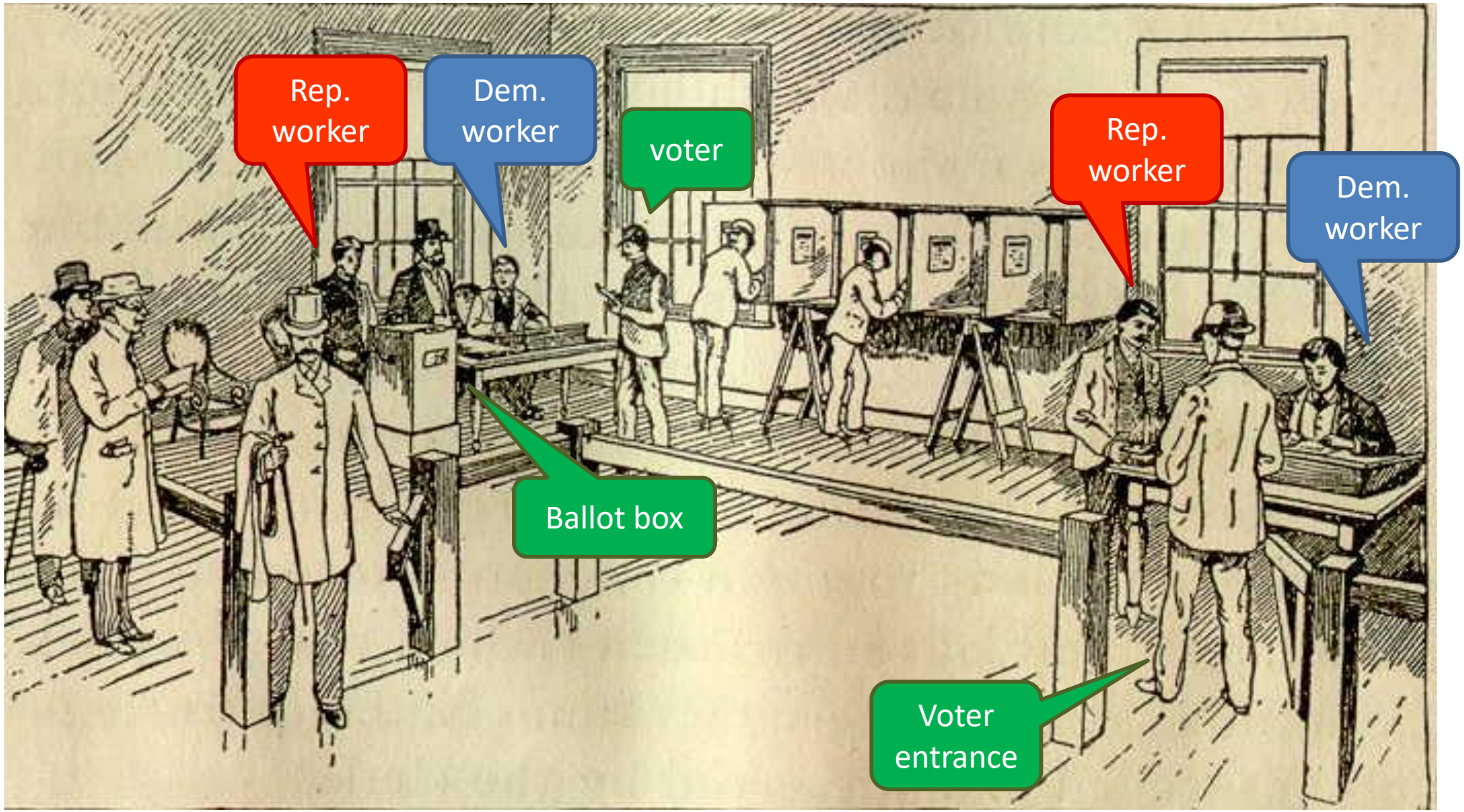
From Elements of Civil Government by Alexander L. Peterman, 1891

Secret Ballots, 1890



From Elements of Civil Government by Alexander L. Peterman, 1891

Secret Ballots, 1890

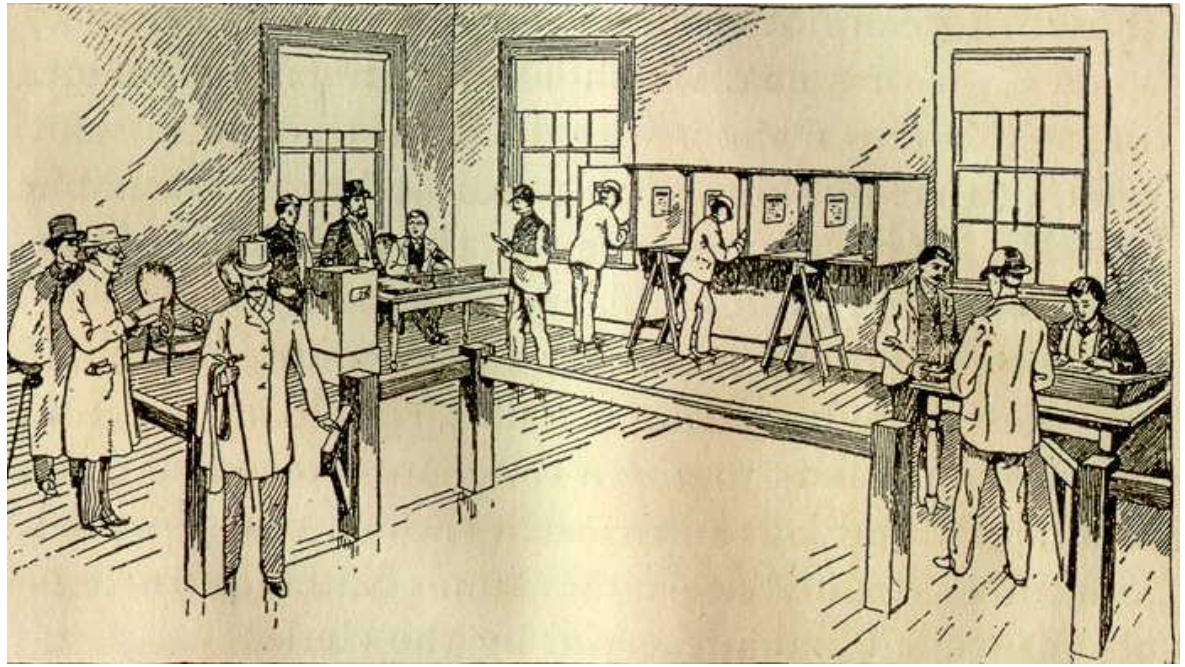


From Elements of Civil Government by Alexander L. Peterman, 1891

Secret Ballots, 1890

Combining Australian ballots with pollbooks, voting booths, and a ballot box that's watched by witnesses from both parties works well

- Parties can trust the results even without trusting each other
- Secrecy
- Can recount the votes



Problems

- Manual counting
- Hard to find volunteers

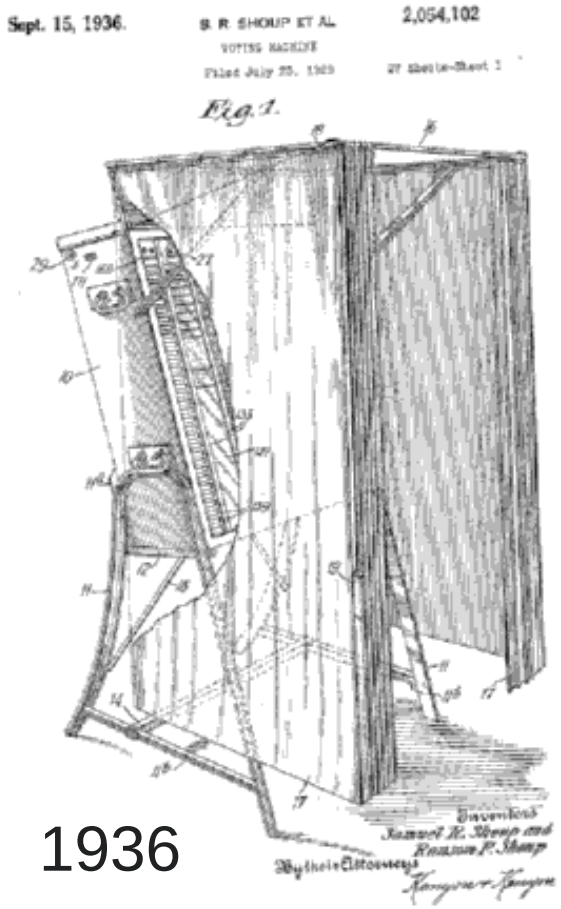
Lever machines, 1890-1990

Simple, fast, accurate counting

Very popular

How do I know my vote counted?

- Cannot recount votes
- Can get rigged



1936

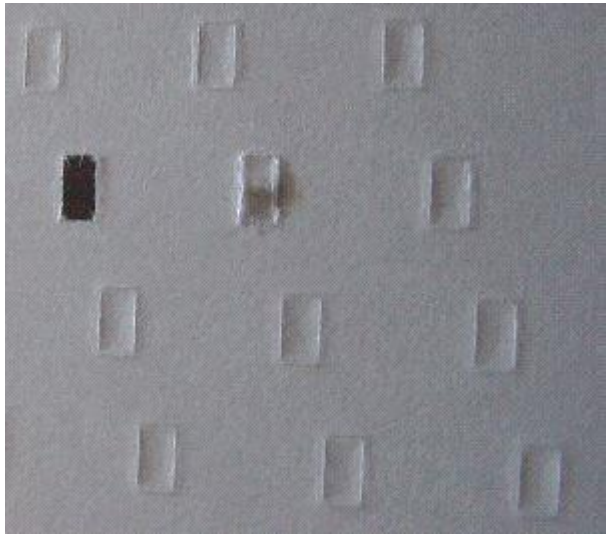
https://homepage.cs.uiowa.edu/~jones/voting/pictures/

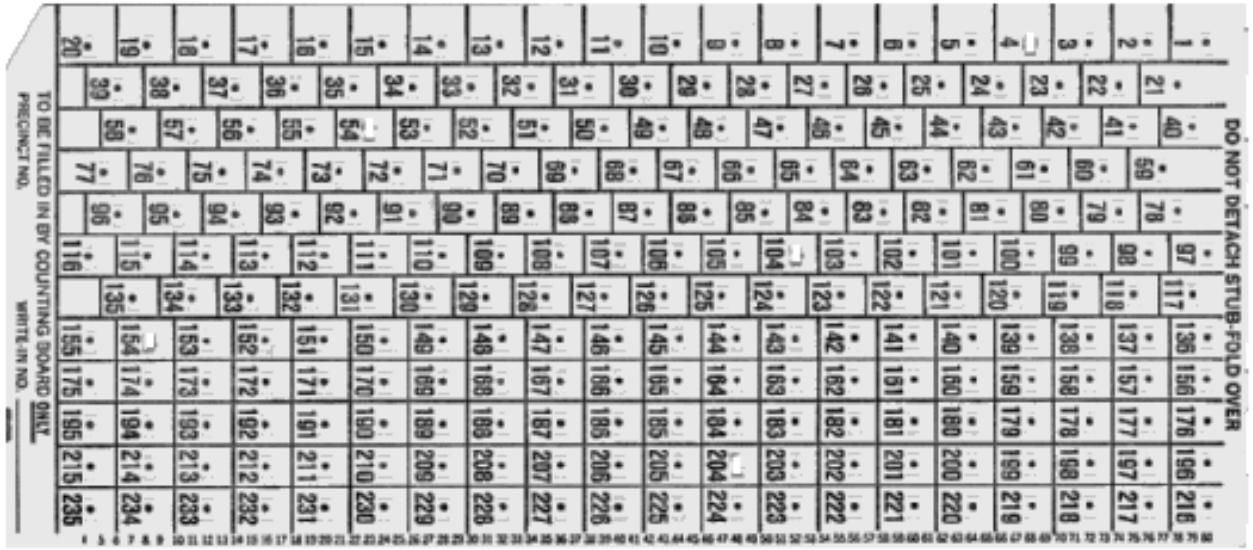
https://news.wbfo.org/post/lever-machines-are-election-history

Punched cards

Initially used in 1890

Gained popularity in the ‘60s with Votomatic

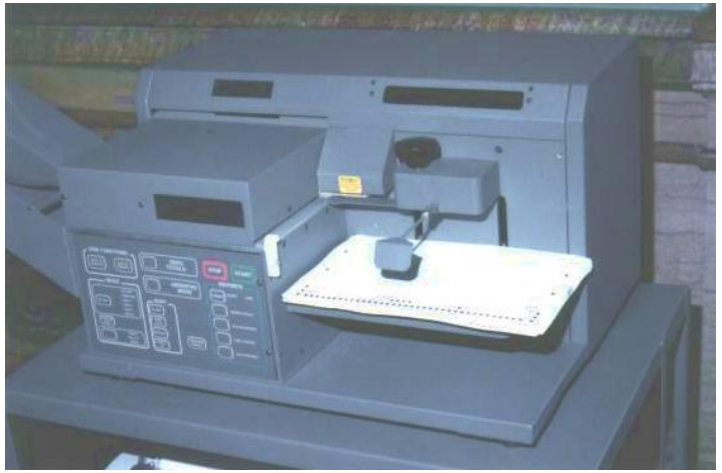


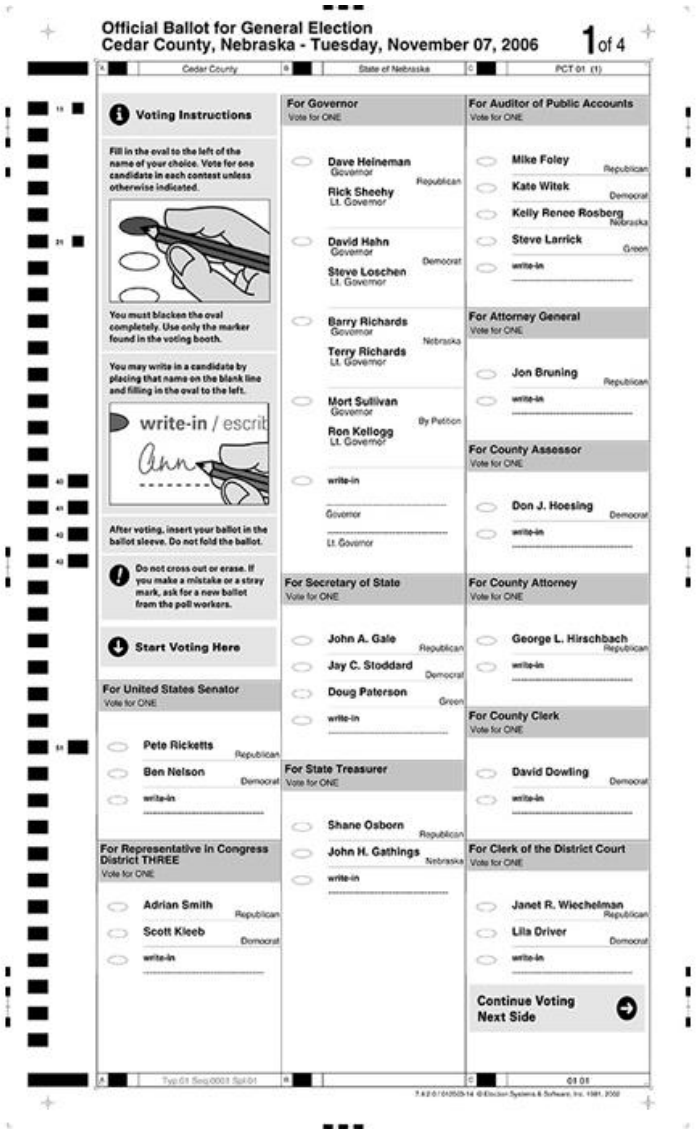


https://homepage.cs.uiowa.edu/~jones/voting/pictures/

Optical scanning 1975

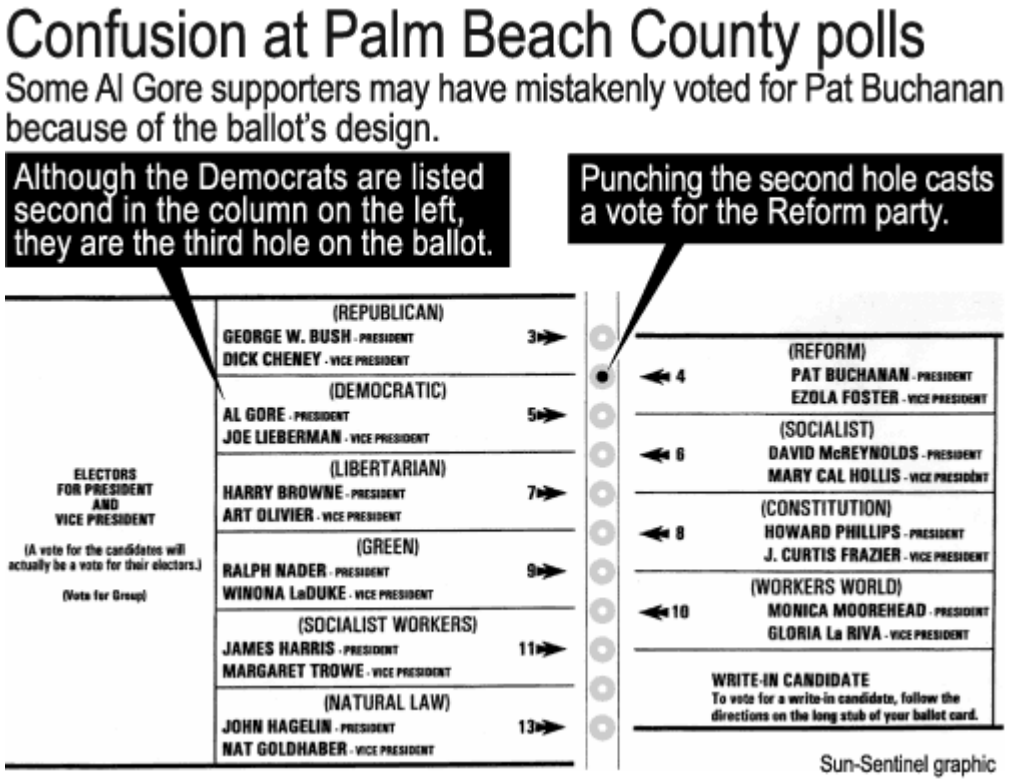
- Efficient tabulation
- Differences in **interpretation** between machine interpretation, and hand interpretation based on “voter intent” rules
- Stray marks (e.g. caused by folds)
- Configuration errors
- Programming errors
- Hacking (adversarial attack)



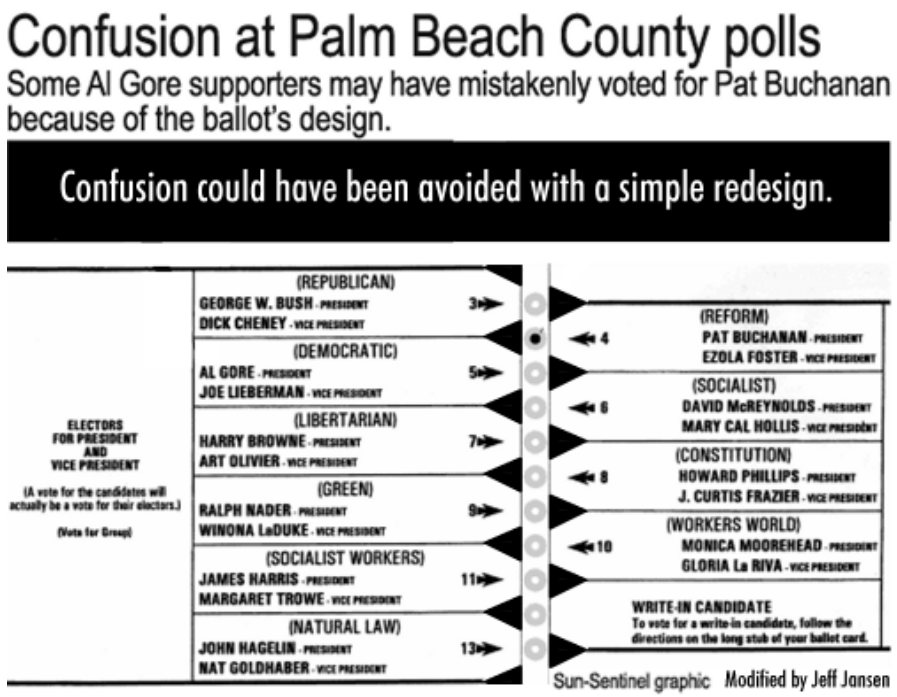


https://homepage.cs.uiowa.edu/~jones/voting/pictures/

Florida 2000



http://www.mit.edu/~jtidwell/ballot_design.html



HAVA - Help America Vote Act (2002)

- 4 Billion dollars allocated
- Mostly to replace voting machines

Touch screen voting machines

- Voter enters its vote and receives a receipt
- No paper trail
- No verifiability: how do I know my vote was counted
- Worse than lever machines:
  - In lever machines a bug/hack always works the same (mechanically)
  - In touch-screen a malicious software can attack only on election day

Diebold AccuVote TS

Sequoia AVC Edge

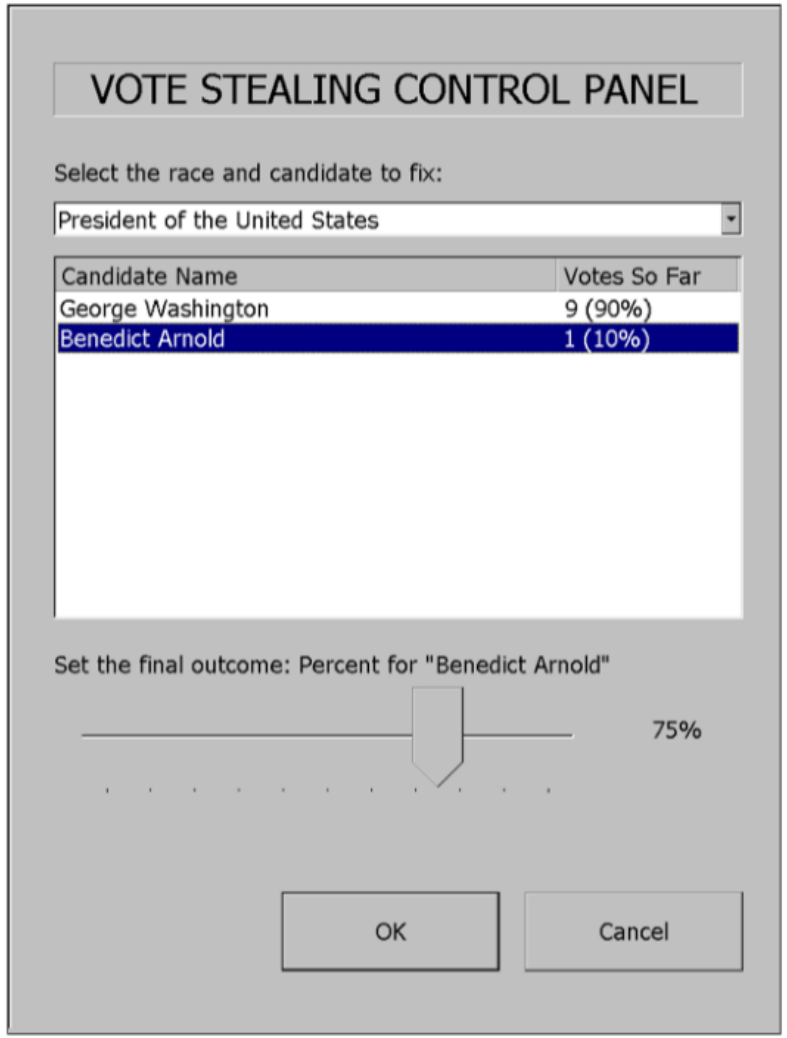
Hart InterCivic eSlate

iVotronic

https://votingmachines.procon.org/how-to-vote-on-an-electronic-voting-machine/

The Princeton Report 2006
[Feldman, Halderman, Felten]

- Demonstrated hacking Diebold touch-screen
- Inserted the malware via memory card (requires 1 minute next to the machine)
- Can spread virally via memory cards
- Prints receipts according to the vote
- Fully determines the outcome (independently of the results)
- All audit logs modified to be consistent



Illustrations

- Hacking Diebold voting machine #1 (2006) https://www.youtube.com/watch?v=5hCyVsUir8k&list=PL07473619B3FA4B21&index=88
- Hacking AVS WINVote machine (2018) https://www.youtube.com/watch?v=CShvCFzjDUU
- Hacking Diebold voting Machine #2 (2018) https://www.inverse.com/article/48038-here-s-how-a-voting-machine-used-in-18-states-can-be-hacked-in-two-minutes
- Playing Pac-Man on Sequoia AVC Edge voting machine (2008) https://www.youtube.com/watch?v=TpMDCArdzwA

Outline

- History of U.S. voting
- Guidelines for secure voting
- Crypto-based voting

What do we want?

- Simple and reliable system
- Voter secrecy
- Quick count
- Transparency (open audit)

What is Transparency?

Anyone can verify that :

- Their vote was **cast as intended**
- The votes were **count as cast**

Paper vs. Electronic

Paper elections:

- Local attacks
- No transparency

Electronic elections today:

- Global attacks
- Undetectable
- Unrecoverable
- No transparency

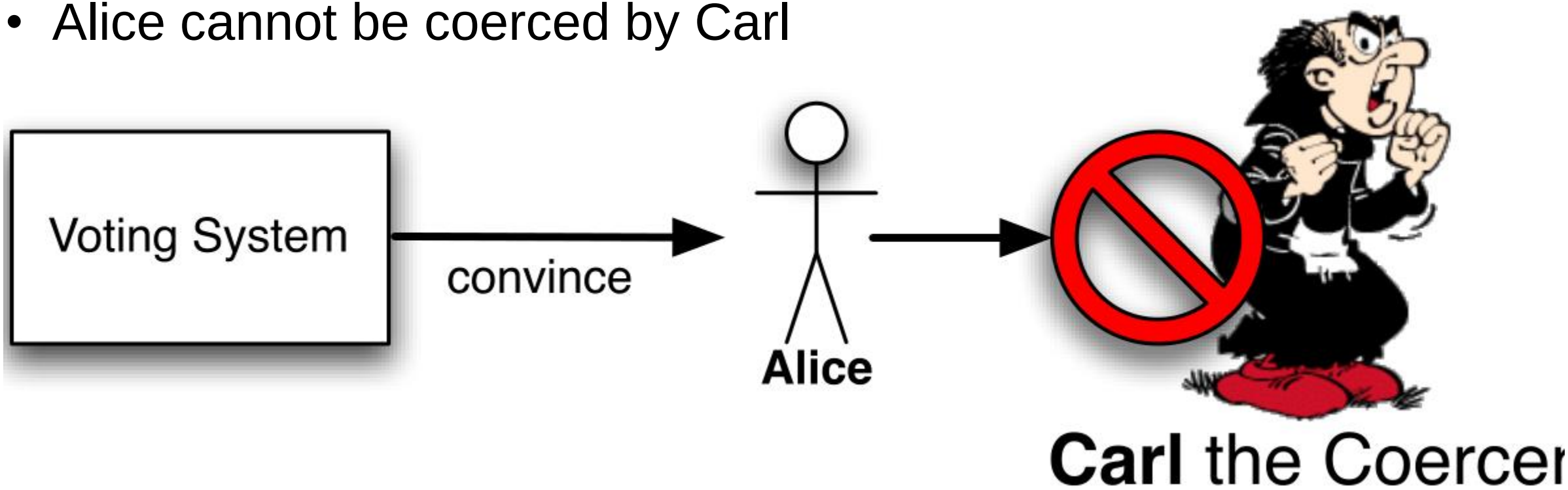
Ideally:

- No local/global attacks
- Full transparency

Secret Ballot vs. Verifiability

Desired Properties

- Alice verifies her vote
- Everyone verifies tallying
- Alice cannot be coerced by Carl



Aviation and Banking?

- Little defense against insiders
- Failures are obvious

- Complete audit logs
- Transferability of claims

https://commons.wikimedia.org/wiki/File:Boeing_777-200ER_(Air_Austral)_7381.jpg

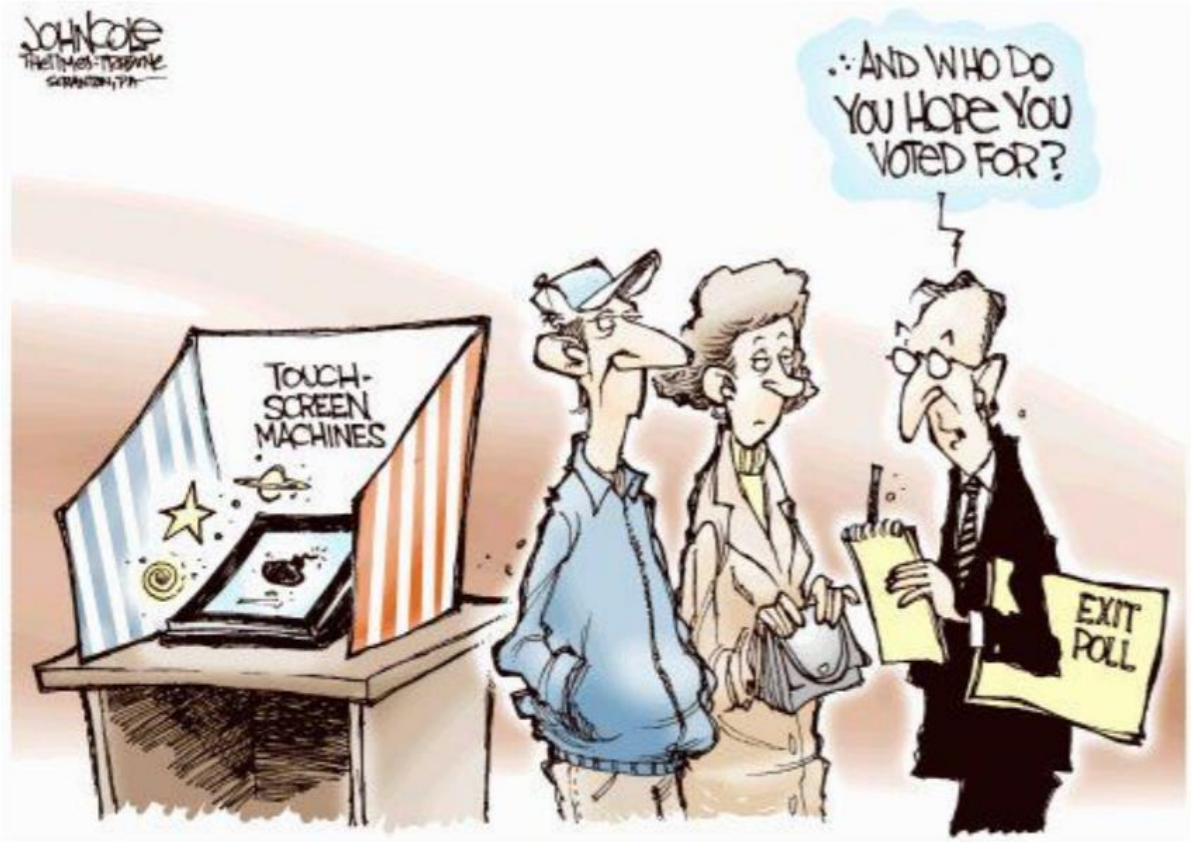
Software Independence [Rivest, Wack'06]

"A voting system is software independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome"

Example

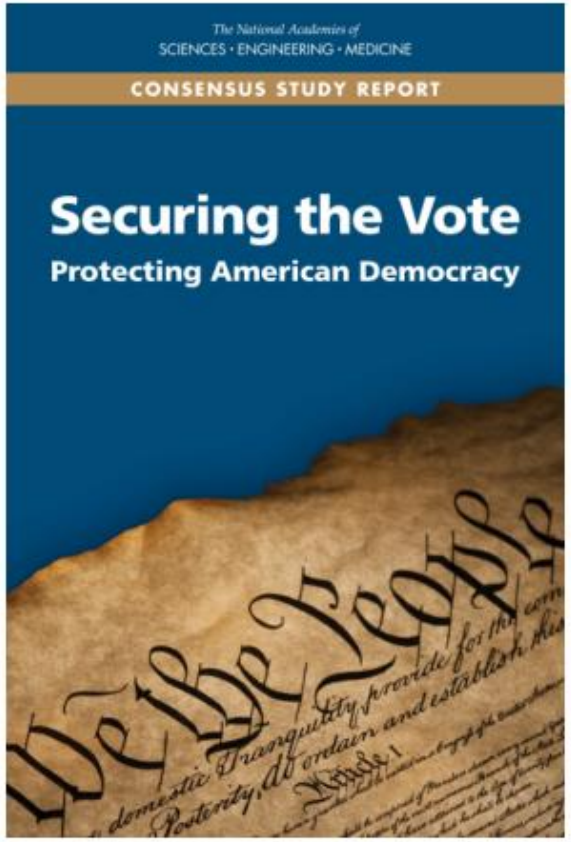
Non-example

Software Independence [Rivest, Wack'06]



And Who Do You Hope You Voted For?

NASEM Report (9/6/18)



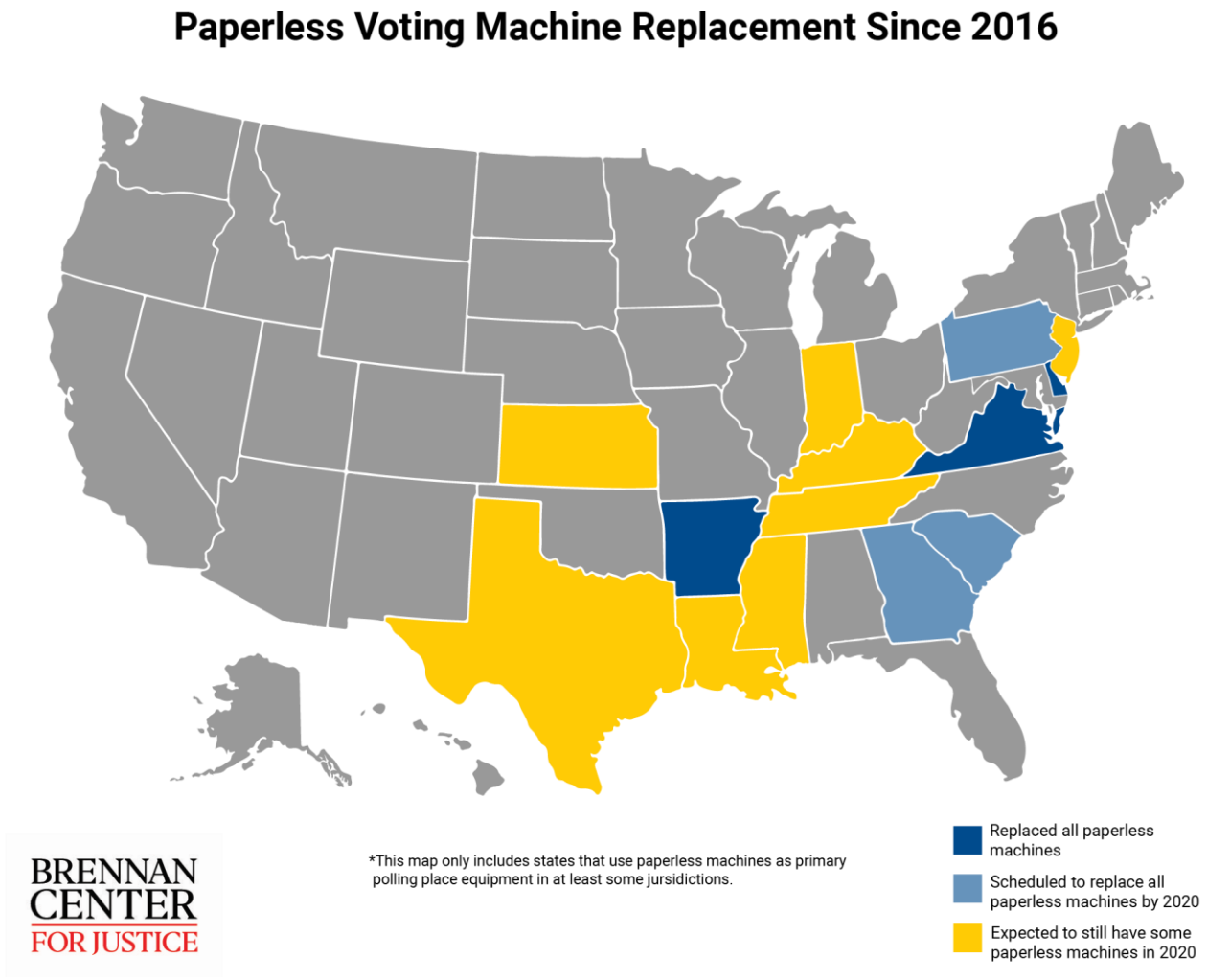
National Academies issued report on
"Securing the Vote"

www.nap.edu/futureofvoting

(159 pages; free pdf)

41 recommendations

Recommendation 4.12:
Use voter verifiable paper ballots everywhere by 2020



Recommendation 5.7-5.9: Audit election outcomes!

Risk Limiting Audit (RLA):

- Sample cast paper ballots at random
- Use statistical methods to analyze the sample
- Get assurance with high probability

Who is audit for?

- **Losing candidates:** to convince them that “they lost fair and square”

“The People have spoken....

the bastards!”

Dick Tuck

1966 Concession Speech

Who is audit for?

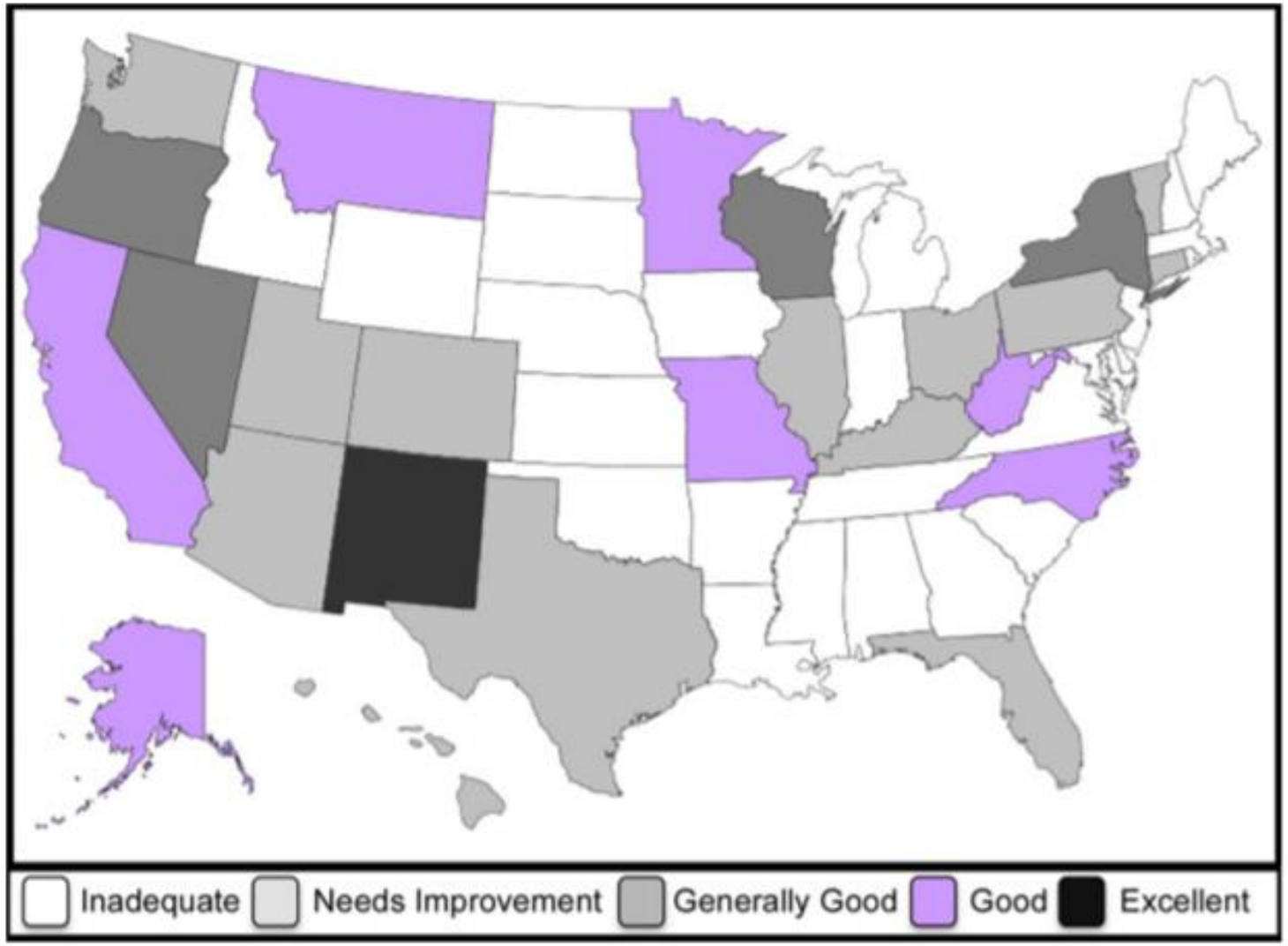
- **Losing candidates:** to convince them that “they lost fair and square”
- **The winner**: to provide a mandate
- **The public**: to assuage doubts about “rigged elections”
- **Election officials**: to help them provide accurate and efficiently-verified results

What a RLA does not do

A RLA does not address:

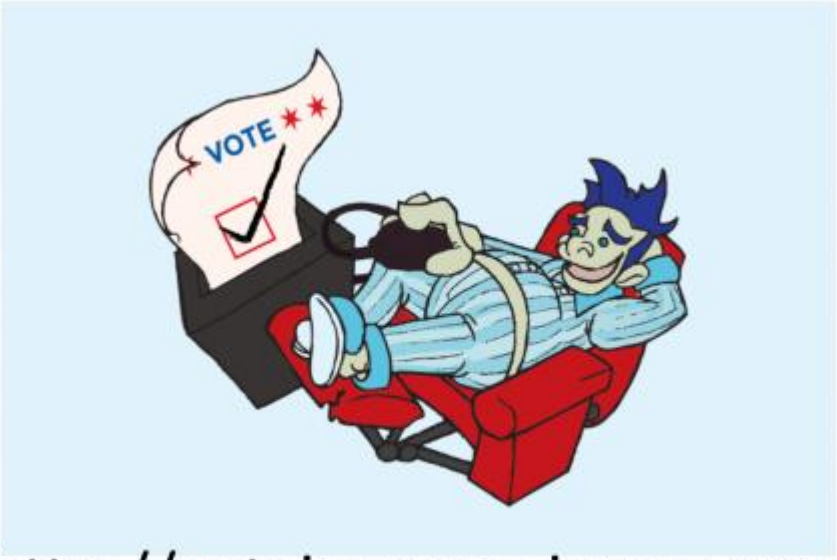
- correctness of the tally (as opposed to the outcome)
- voter eligibility
- voter authentication
- usability
- privacy
- chain of custody of paper ballotsv

Post-Election Audit



https://www.eac.gov/sites/default/files/eac_assets/1/28/VerifiedVoting-Post-Election-Audits.pdf

Recommendation 5.11: No Internet voting!



http://voteinyourpajamas.org/

Outline

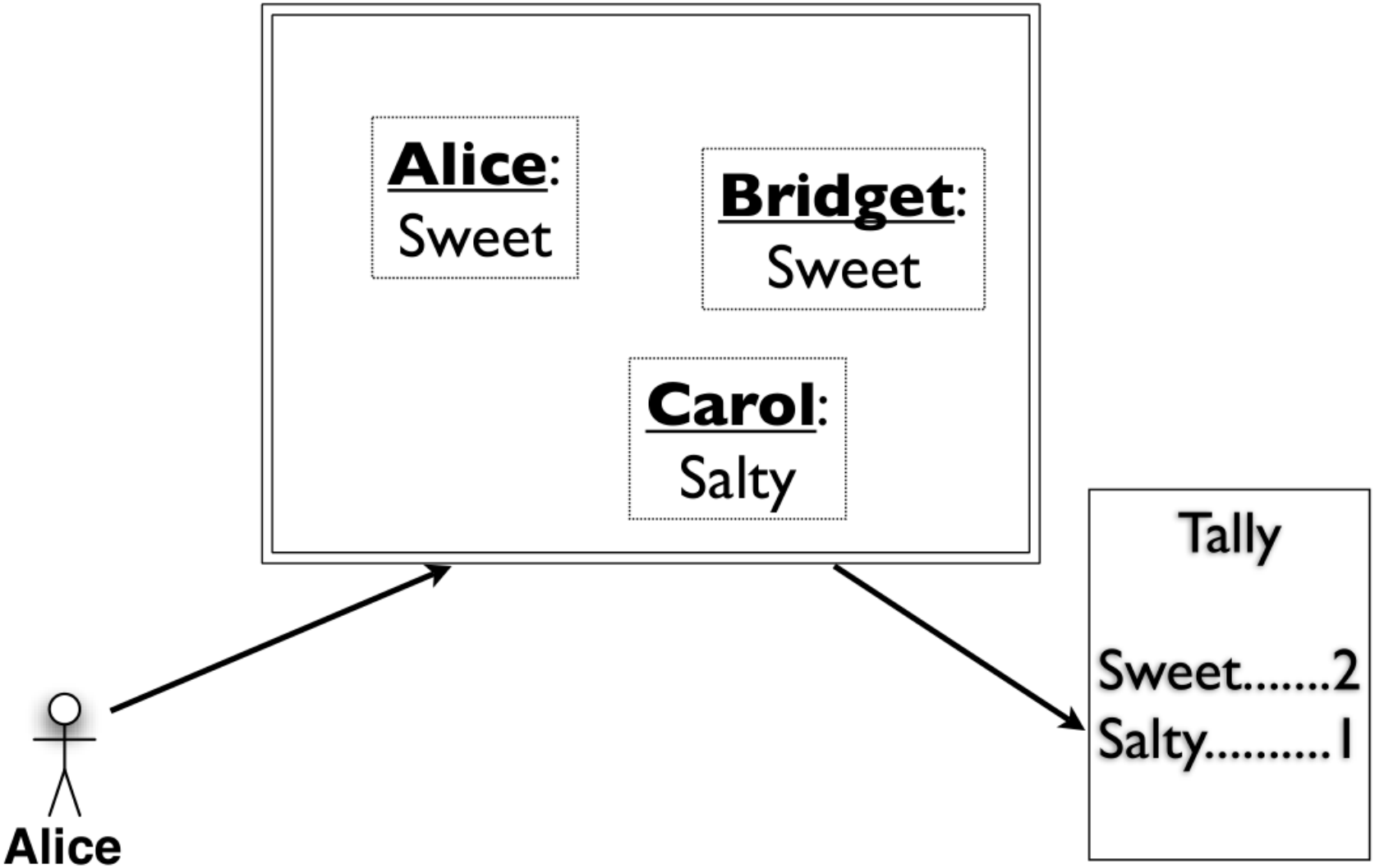
- History of U.S. voting
- Guidelines for secure voting
- Crypto-based voting

Recall

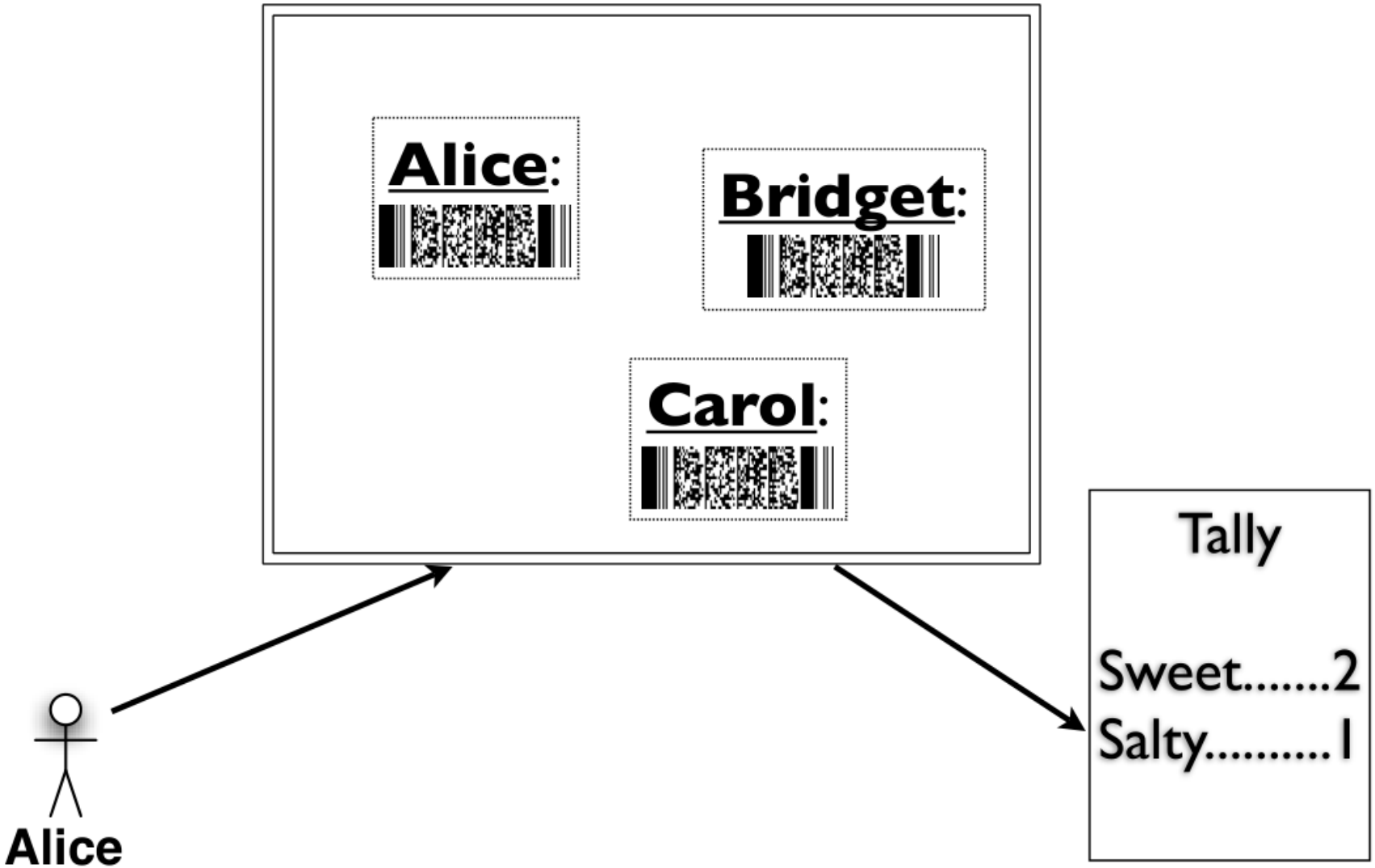
This system is not private, but can provide good verifiability

Can emulate it with privacy?

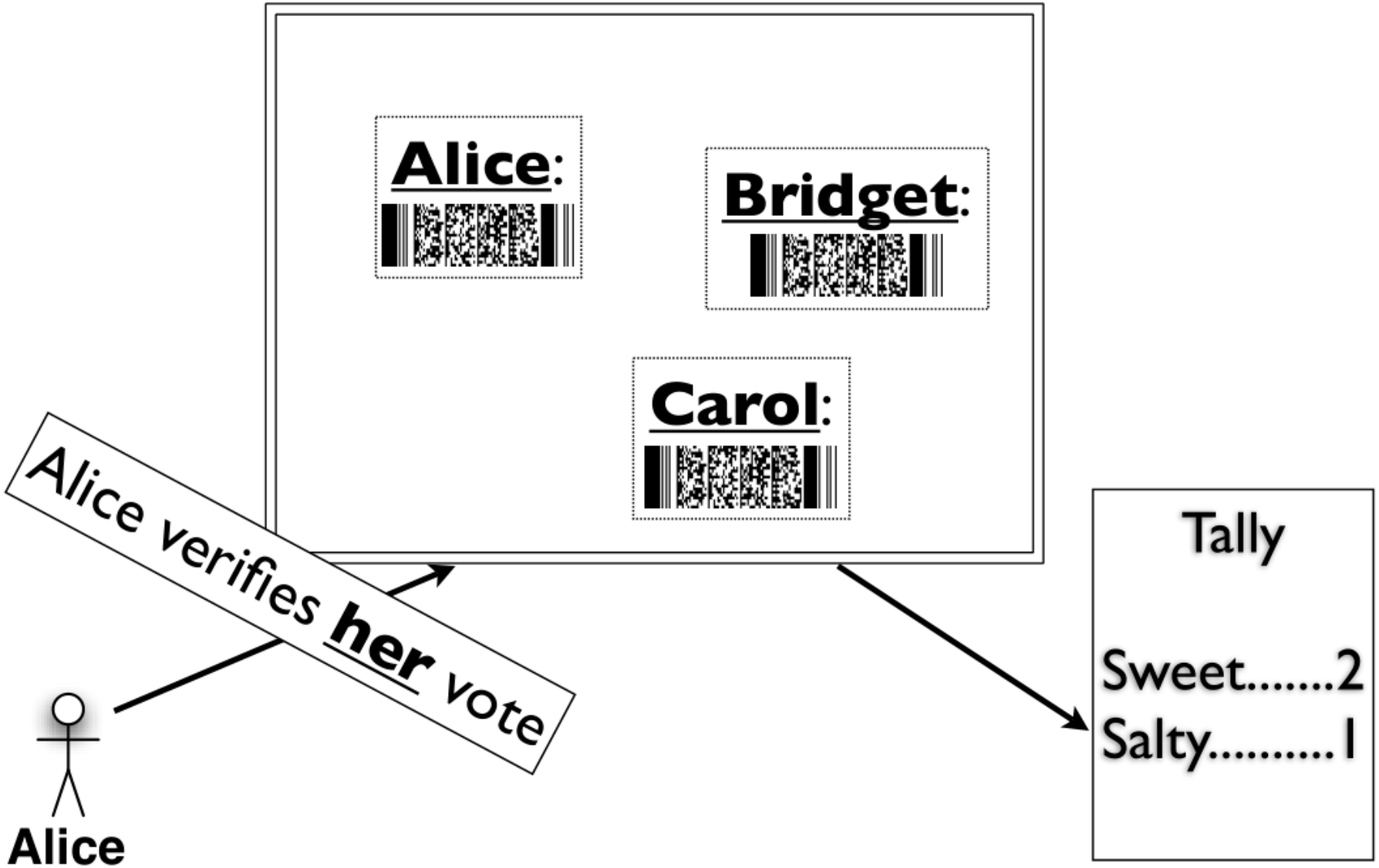
Public Ballots



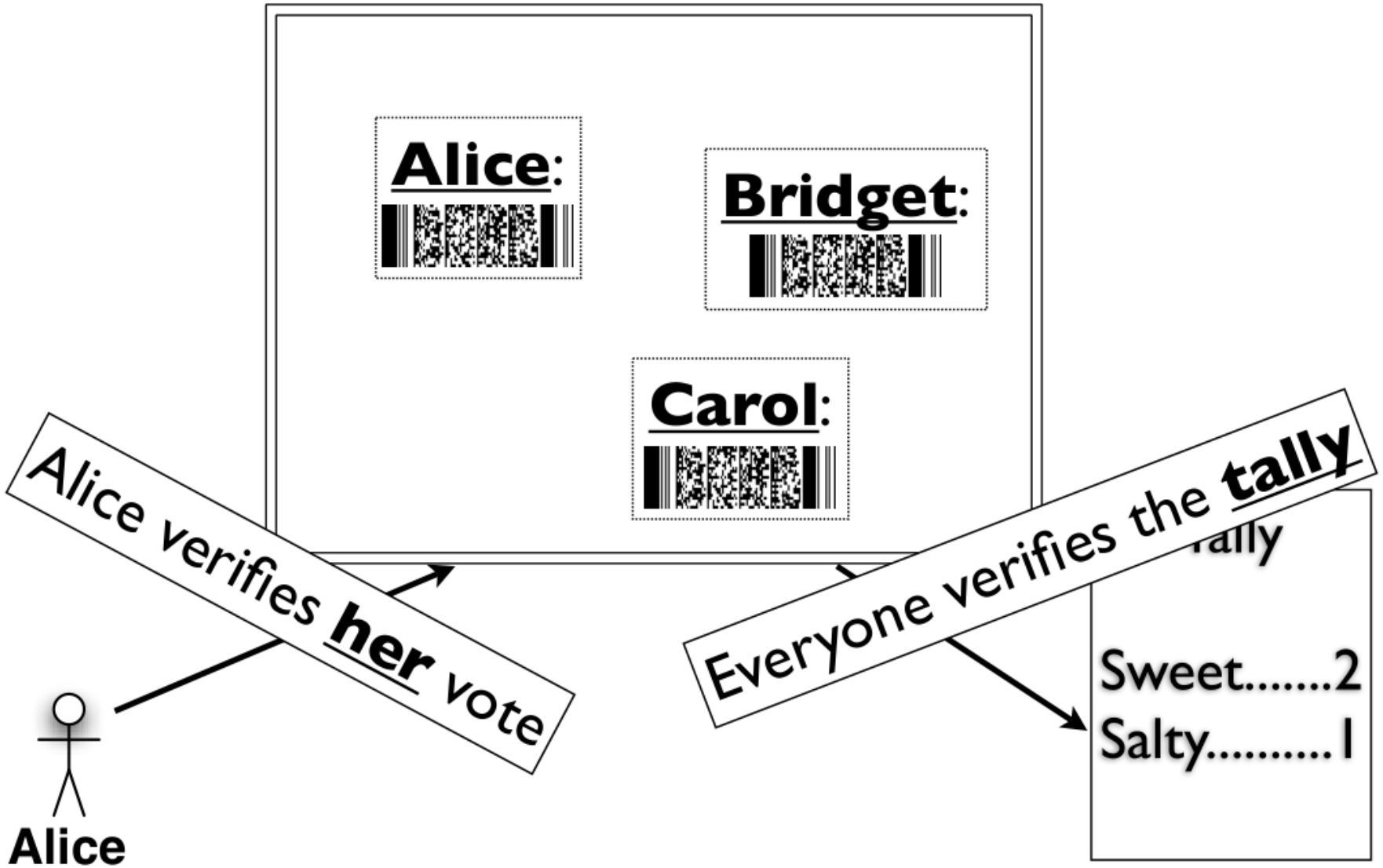
Encrypted Public Ballots



Encrypted Public Ballots



Encrypted Public Ballots



Additively Homomorphic Public-Key Encryption

We want a PKE that supports

$$Enc_{pk}(m_1) \cdot Enc_{pk}(m_2) = Enc_{pk}(m_1 + m_2)$$

E.g., textbook RSA provide multiplicative homomorphism

- $Enc_{pk}(m_1) = m_1^e (\mathrm{mod}\ N)$
- $Enc_{pk}(m_2) = m_2^e (\mathrm{mod}\ N)$
- $Enc_{pk}(m_1) \cdot Enc_{pk}(m_2) = m_1^e \cdot m_2^e (\mathrm{mod}\ N) = (m_1 \cdot m_2)^e (\mathrm{mod}\ N)$

This allows everyone to sum the votes and get an encrypted count

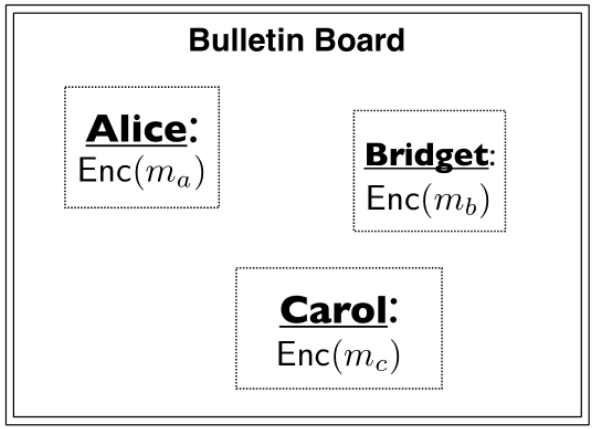
Additively Homomorphic Public-Key Encryption

- Alice can verify her vote is counted
- Everyone can sum all votes
- Magic sauce: Zero-knowledge proofs
- Can prove statements on the plaintext w/o revealing anything else about it

$$\mathsf{Enc}(m_1) \times \mathsf{Enc}(m_2) = \mathsf{Enc}(m_1 + m_2)$$

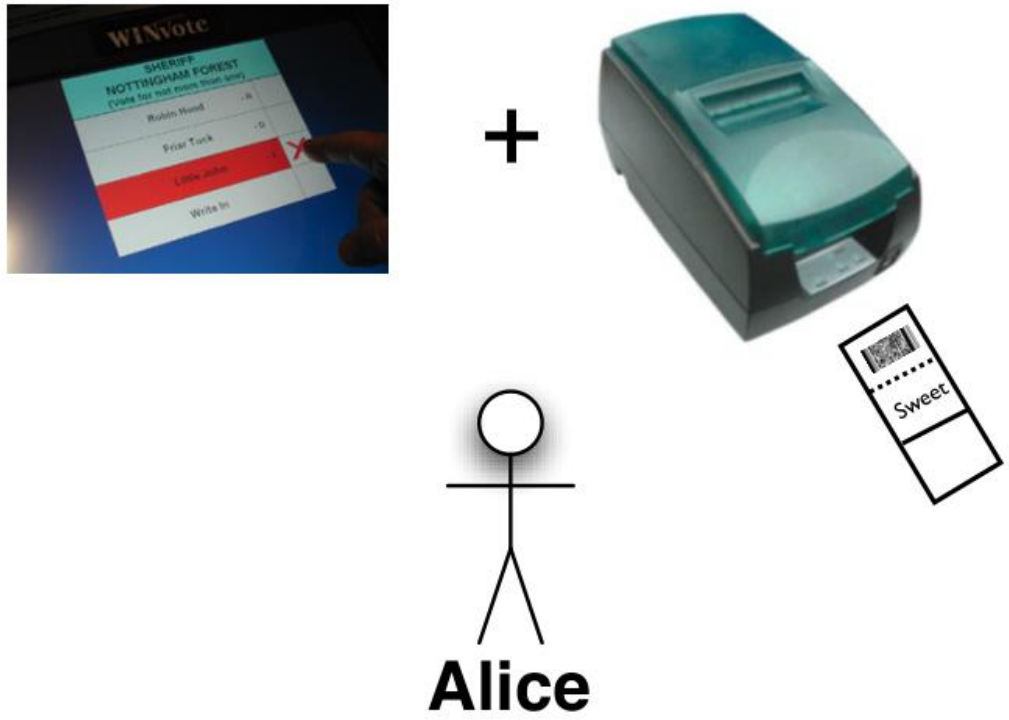
$$\mathsf{Yes} = \mathsf{Enc}(1)$$

$$\mathsf{No} = \mathsf{Enc}(0)$$



$$\mathsf{EncryptedTally} = \mathsf{Enc}(m_a) \times \mathsf{Enc}(m_b) \times \mathsf{Enc}(m_c) = \mathsf{Enc}(m_a + m_b + m_c)$$

Encrypted Public Ballots



Encrypted Public Ballots