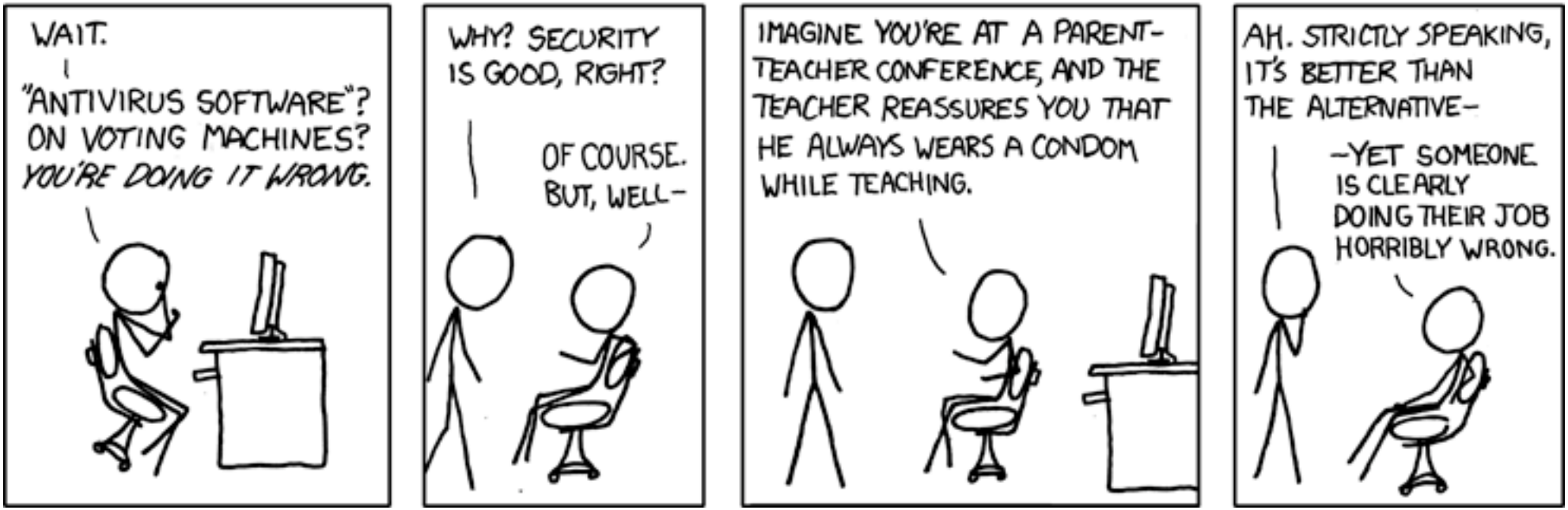
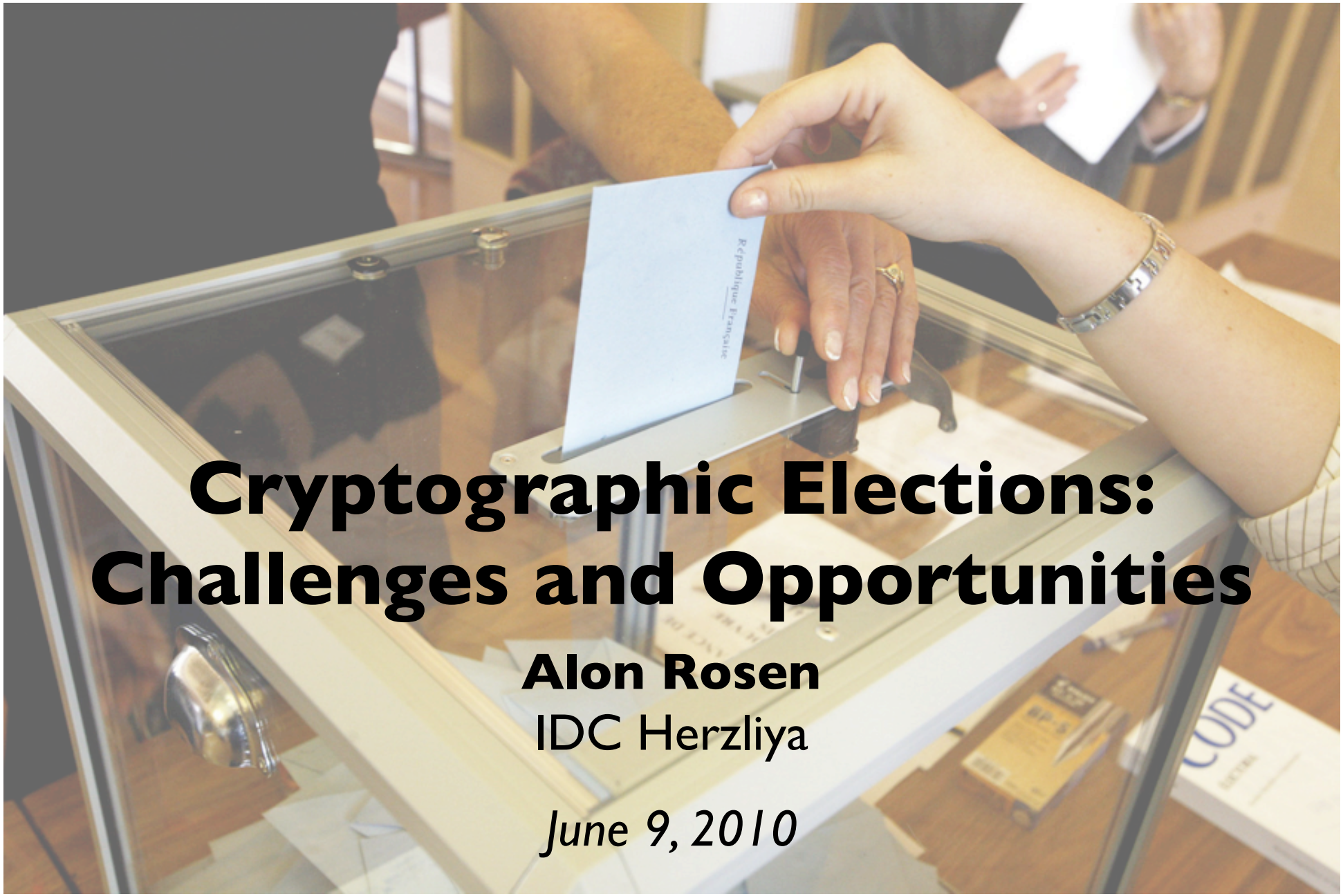
PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD) HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.





Cryptographic Elections: Challenges and Opportunities

Alon Rosen
IDC Herzliya

June 9, 2010

Thanks

- Ben Adida (Harvard University)
- Yuval Kedem (Gallileo)
- David Movshovitz (IDC Herzlyia)
- Shimon Schocken (IDC Herzlyia)
- Amnon Ta-Shma (Tel Aviv University)

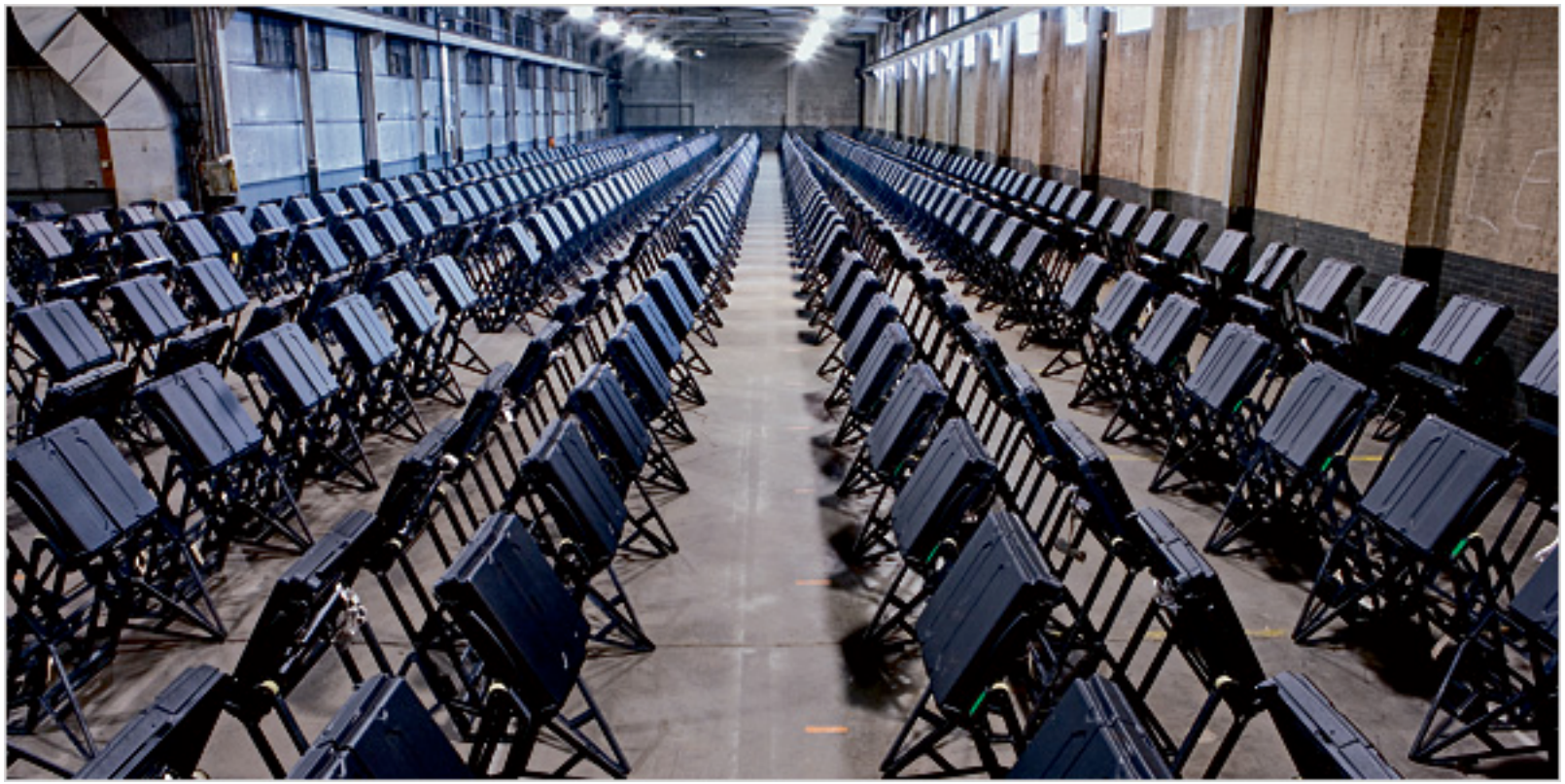
This Talk

<u>Part I</u>

- ➡ Electronic voting in US
- ➡ The Israeli perspective

<u>Part II</u>

- ➡ Why is voting so hard?
- ➡ Cryptographic voting.

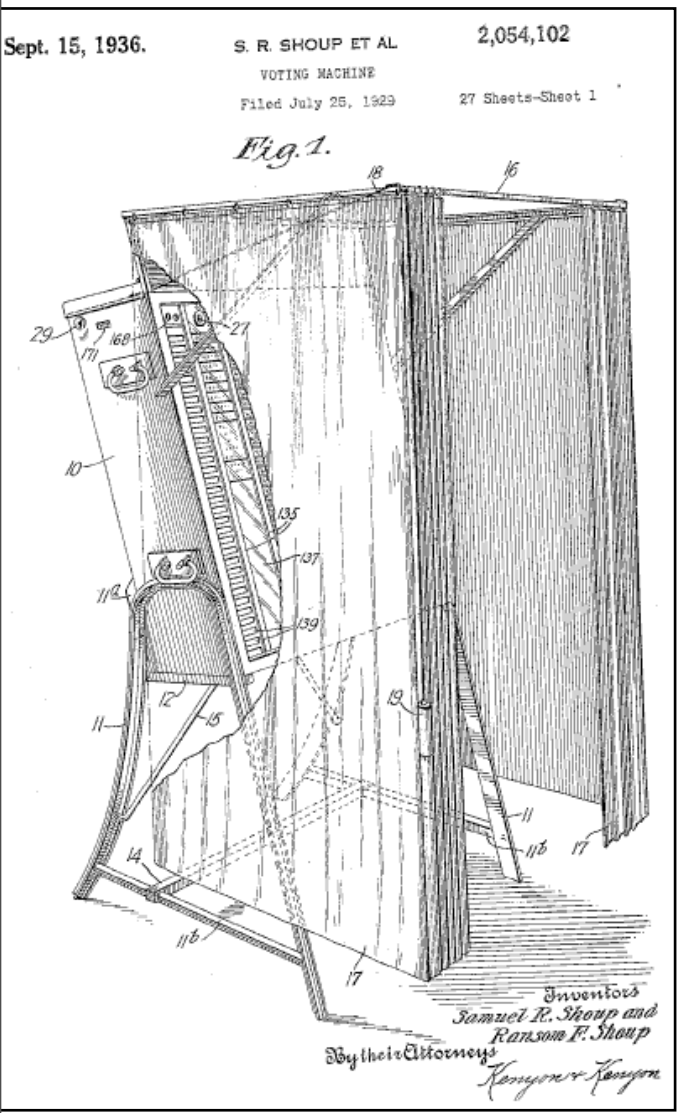


http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html

Voting in the US

http://www.cs.uiowa.edu/~jones/voting/pictures/

Voting in the US

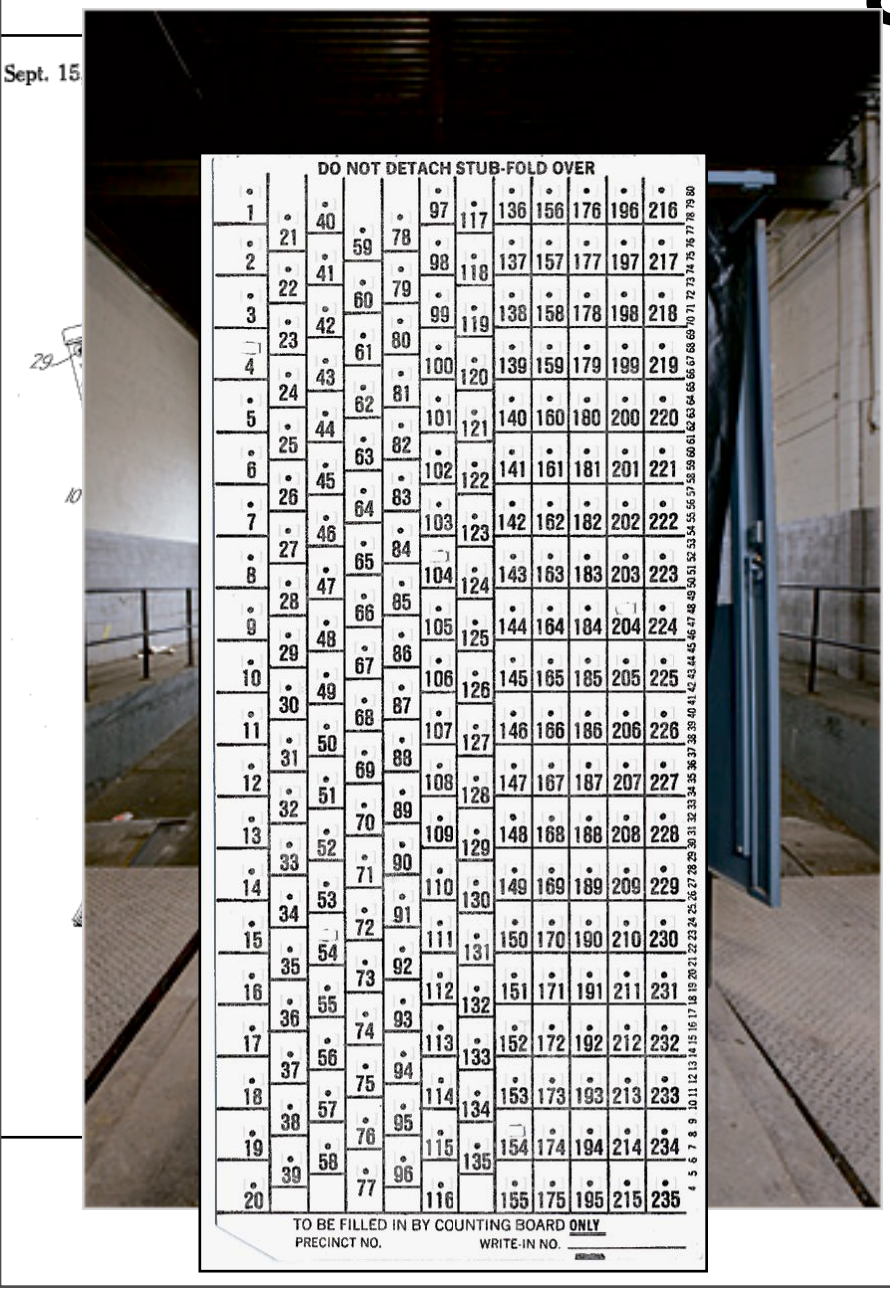


http://www.cs.uiowa.edu/~jones/voting/pictures/

Voting in the US

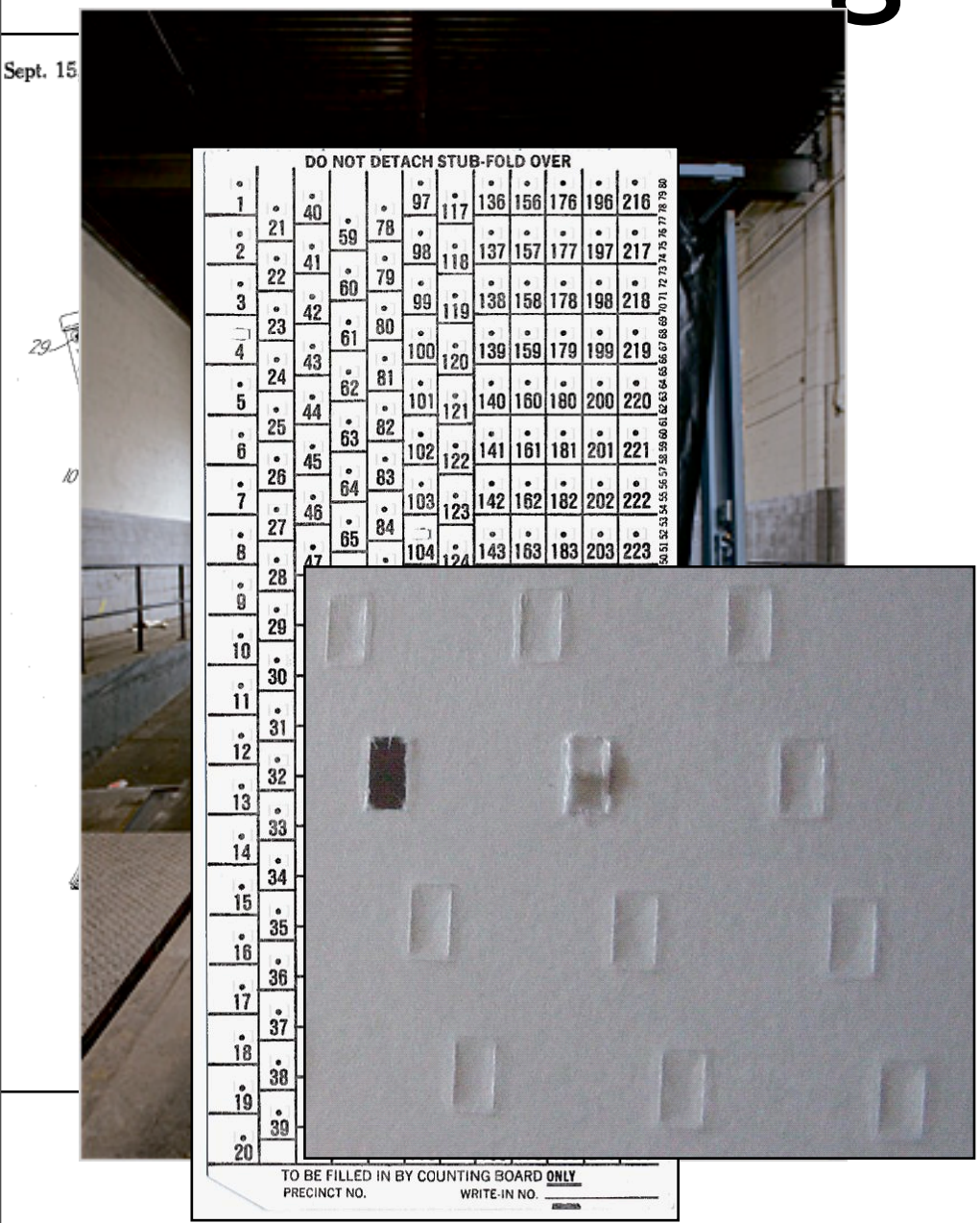
http://www.cs.uiowa.edu/~jones/voting/pictures/

Voting in the US



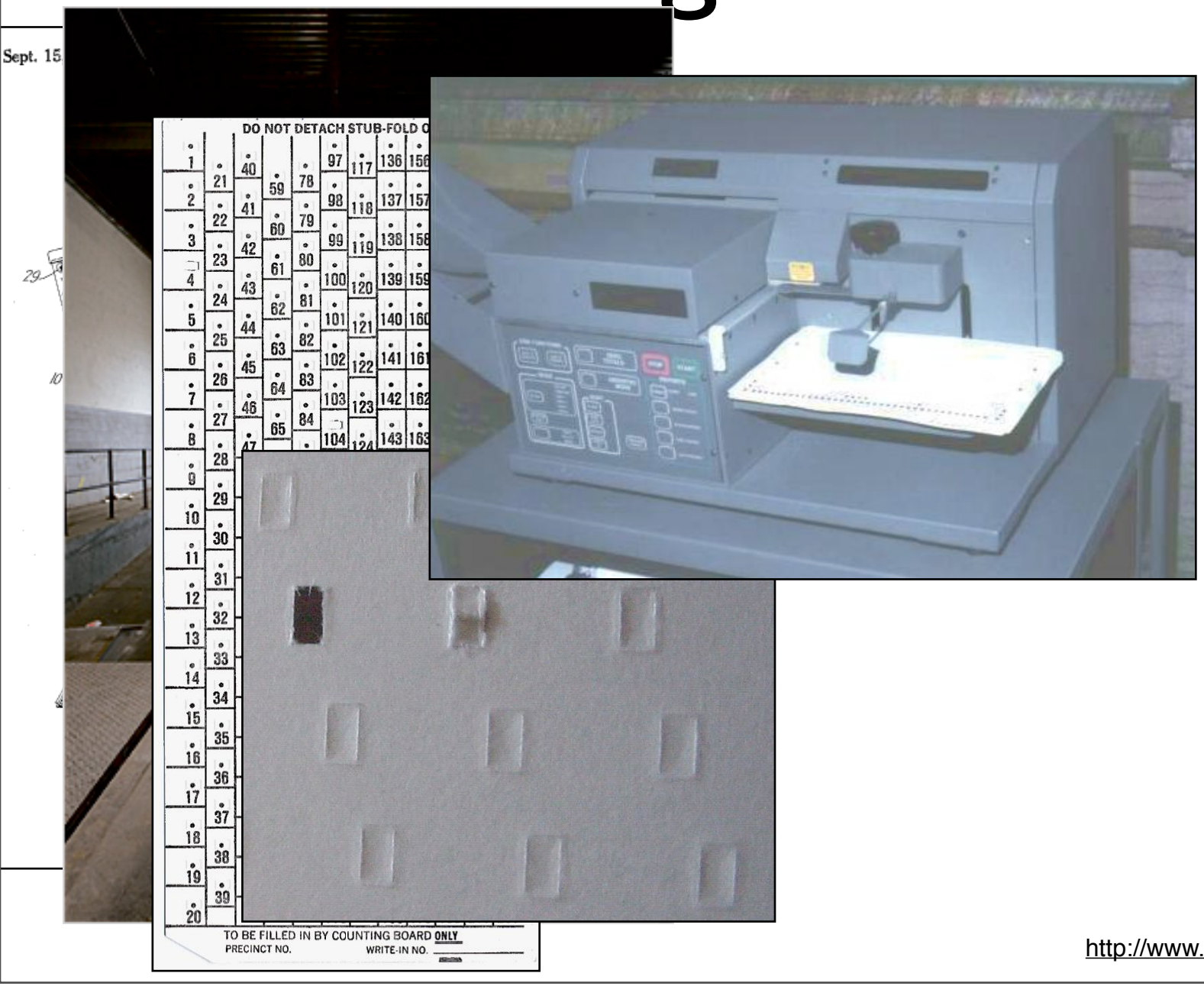
http://www.cs.uiowa.edu/~jones/voting/pictures/

Voting in the US



http://www.cs.uiowa.edu/~jones/voting/pictures/

Voting in the US

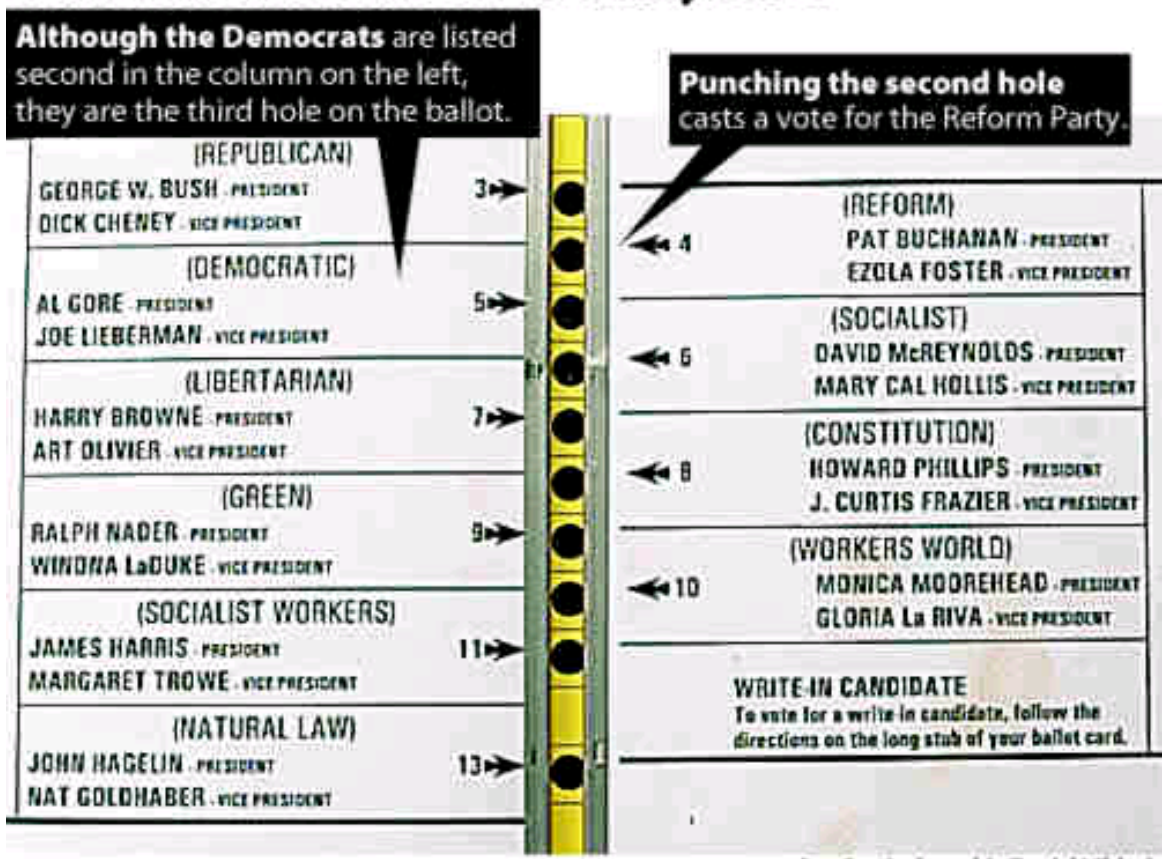


http://www.cs.uiowa.edu/~jones/voting/pictures/

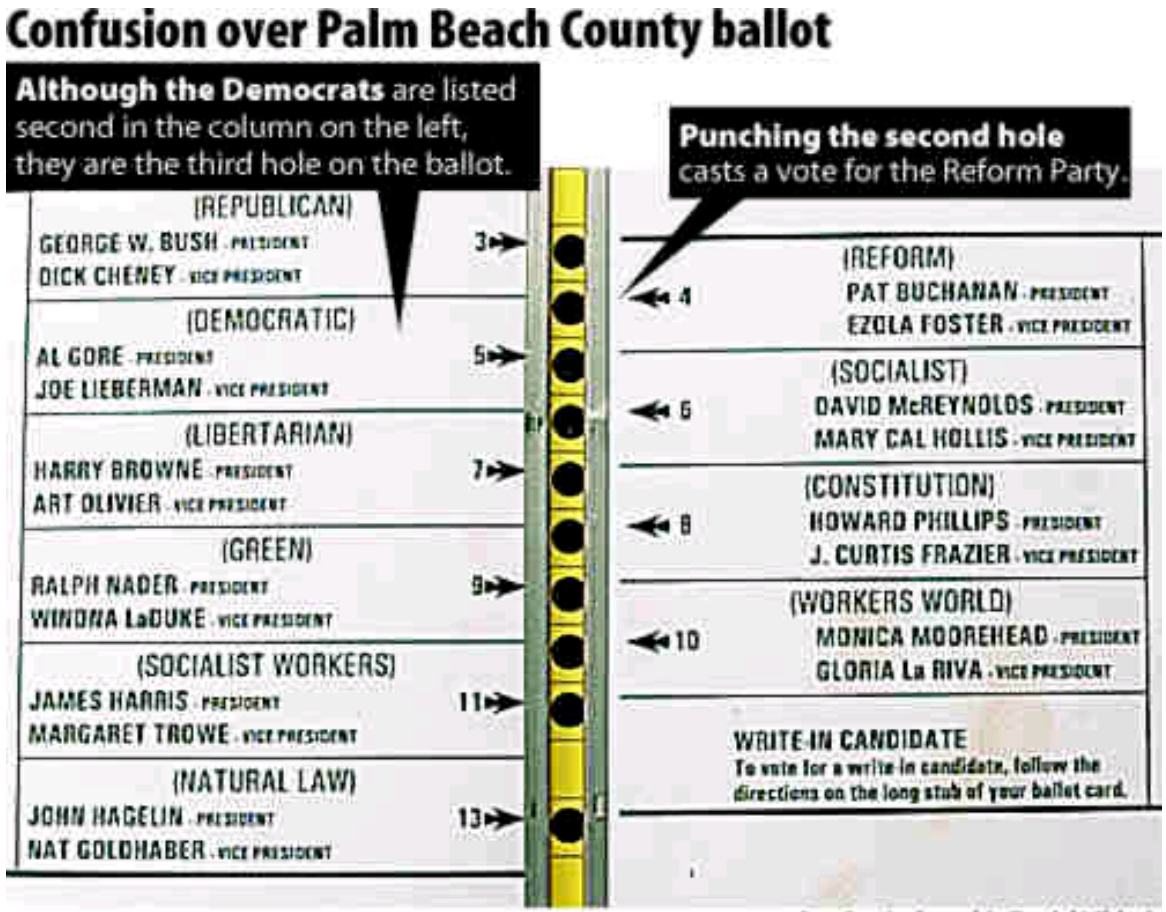
Voting in the US

http://www.cs.uiowa.edu/~jones/voting/pictures/

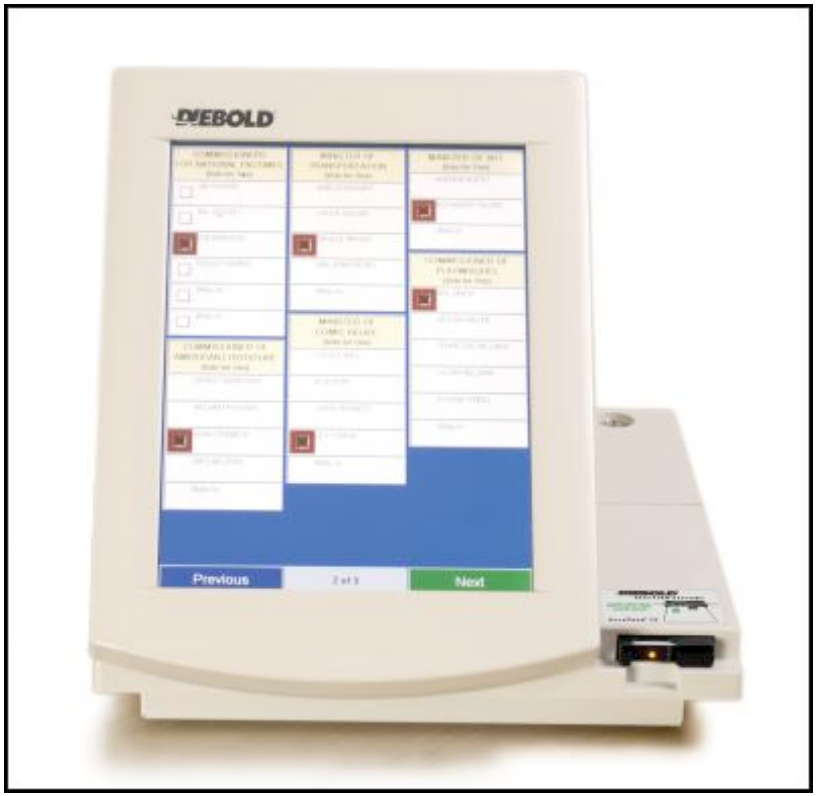
Confusion over Palm Beach County ballot



Sun-Sentinel graphic/Daniel Niblock

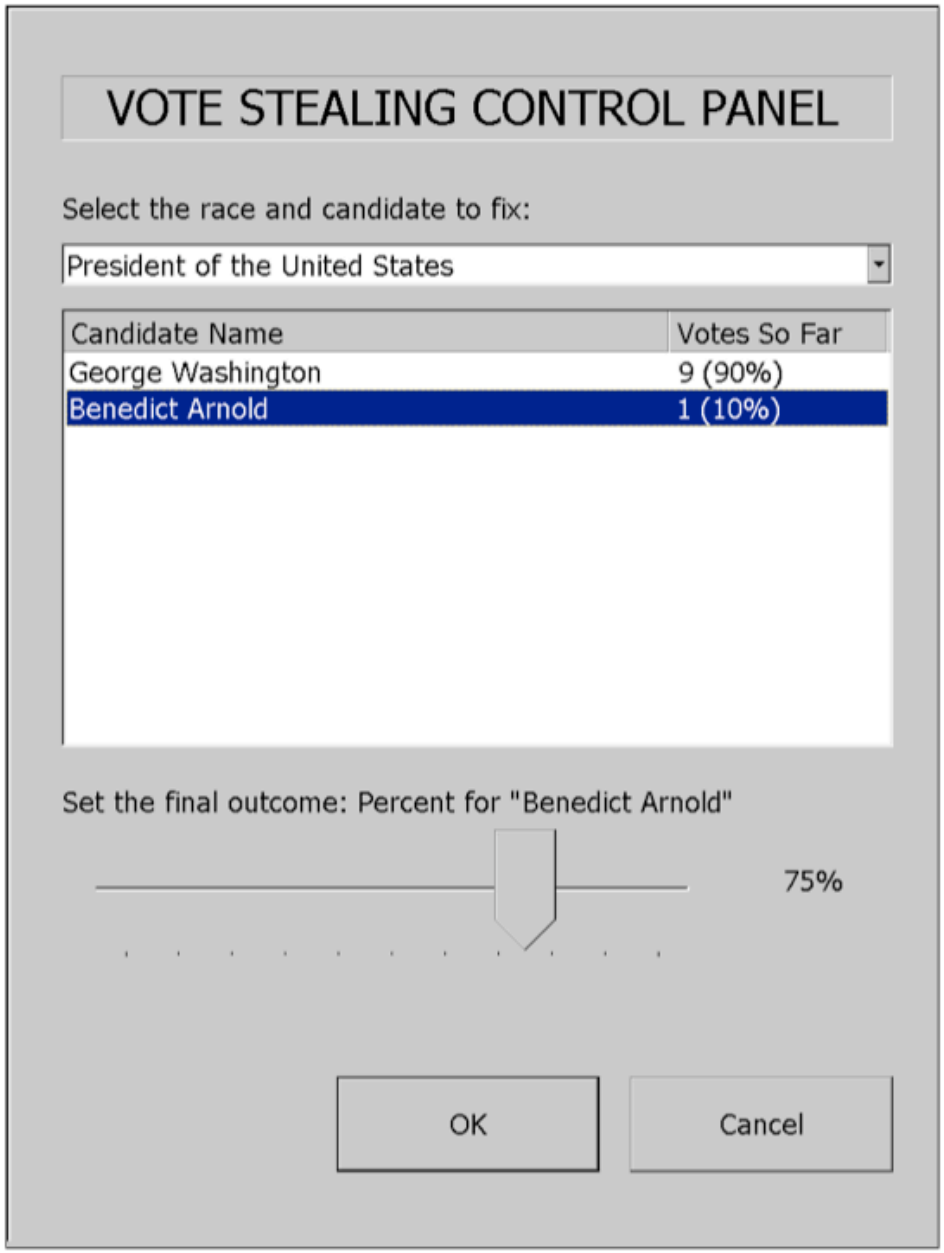


- HAVA - Help America Vote Act
- 4 Billion dollars allocated
- Mostly to replace voting machines



- HAVA - Help America Vote Act
- 4 Billion dollars allocated
- Mostly to replace voting machines

The Princeton Report



- Diebold touch-screen runs executable code loaded from memory card
- All audit logs modified to be consistent
- Can spread virally by memory card.

[FHF2006]

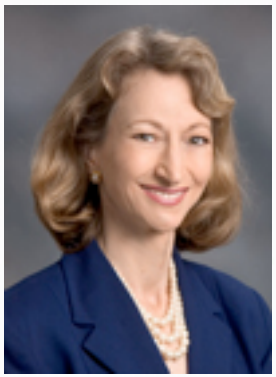
- New Mexico (March 2006)
- California (August 2007)
- Florida (December 2007)
- Ohio (January 2008)
- Iowa (March 2008)
- ...

- States that mandate paper trail.

State of California

SECRETARY OF STATE

**WITHDRAWAL OF APPROVAL OF
DIEBOLD ELECTION SYSTEMS, INC.,
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS
DRE & OPTICAL SCAN VOTING SYSTEM
AND CONDITIONAL RE-APPROVAL OF
USE OF DIEBOLD ELECTION SYSTEMS, INC.,
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS
DRE & OPTICAL SCAN VOTING SYSTEM**



Debra Bowen

State of California

SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & OPTICAL SCAN VOTING SYSTEM

What does Everbody Want?

- Simple and reliable system
- Voter secrecy
- Quick count

- And in addition: transparency (open audit).

What is Transparency?

<u>Anyone can verify that:</u>

- their vote was **<u>cast as intended</u>**
- the votes were **<u>count as cast</u>**

Paper vs. Electronic

Paper elections:

- Local attacks
- No transparency

Electronic elections today:

- Global attacks
- Undetectable
- Unrecoverable
- No transparency

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

Aviation and Banking?

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

- Little defense against insiders

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

- Little defense against insiders
- Failures are obvious

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

- Little defense against insiders
- Failures are obvious

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

- Little defense against insiders
- Failures are obvious

- Complete audit logs

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

- Little defense against insiders
- Failures are obvious

- Complete audit logs
- Transferability of claims

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Aviation and Banking?

- Little defense against insiders
- Failures are obvious

- Complete audit logs
- Transferability of claims

These are poor analogies.

http://commons.wikimedia.org/wiki/Image:738100.jpg

http://www.sxc.hu/photo/206579

Open-Source?

THE HOLLYWOOD HILL

Invites you to

TOWARDS "WE.GOV"

RESTORING TRUST IN OUR ELECTIONS SYSTEMS

an exclusive presentation and discussion with the

OPEN SOURCE DIGITAL VOTING FOUNDATION

and special guests

California Secretary of State Debra Bowen

Technology Entrepreneur Mitch Kapor

RockTheVote Exec Director Heather Smith

Registrar-Recorder for L.A County Dean Logan

Wednesday, October 21st, 2009 | 7:00 – 10:00 pm

Residence of Film Producer Lawrence Bender in Bel Air, CA.

By Invitation Only. Cocktails, Hors D'oeuvres, Valet Parking.
For special requests, email Paris@hhill.org

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"

Examples

http://www.youtube.com/watch?v=zeHmsrLc4jc

Examples

http://www.youtube.com/watch?v=zeHmsrLc4jc

Non-example


JUSTIÇA
ELEITORAL
Lei nº 10.826, de 22/12/2003
O comércio de armas de
fogo e munição deve ser
proibido no Brasil?
1 - SIM
2 - NÃO
1 2 3
4 5 6
7 8 9
0
BRANCO
CORRIGE
CONFIRMA
PROCOMP

The Israeli Perspective

- Nov ’07: Pilot of electronic voting with touch screens in several municipalities.
- Nov ’07: Minister of interior announces plan to move to electronic elections
- Apr ’08: TEHILA are given mandate to run pilot in 3 municipalities.
- Sep’08 - today: Legislation underway to accommodate pilot.

The process:

- No public scrutiny
- No open design

The result:

- No paper trail
- No software independence

Why is Voting so Hard?

The Point of An Election

"The People have spoken....
the bastards!"

Dick Tuck
1966 Concession Speech

The Point of An Election

"The People have spoken....
the bastards!"

Dick Tuck
1966 Concession Speech

Provide enough evidence
to convince the loser.

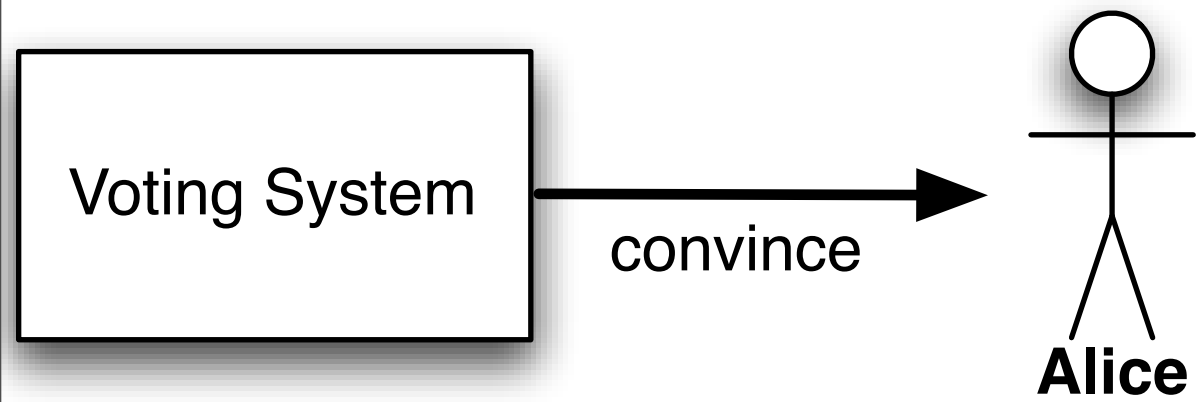
http://www.cs.uiowa.edu/~jones/voting/pictures/

Secret Ballot *vs.* Verifiability

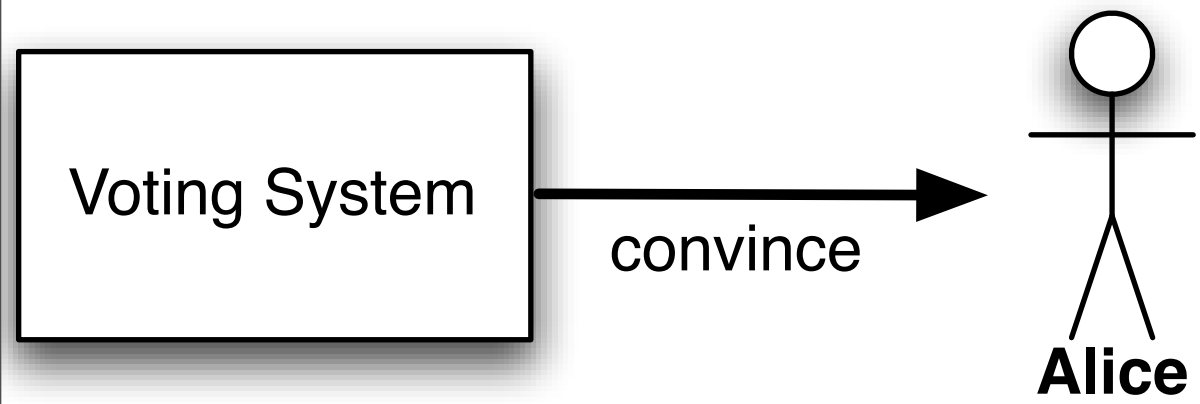
Secret Ballot *vs.* Verifiability

Voting System

Secret Ballot *vs.* Verifiability

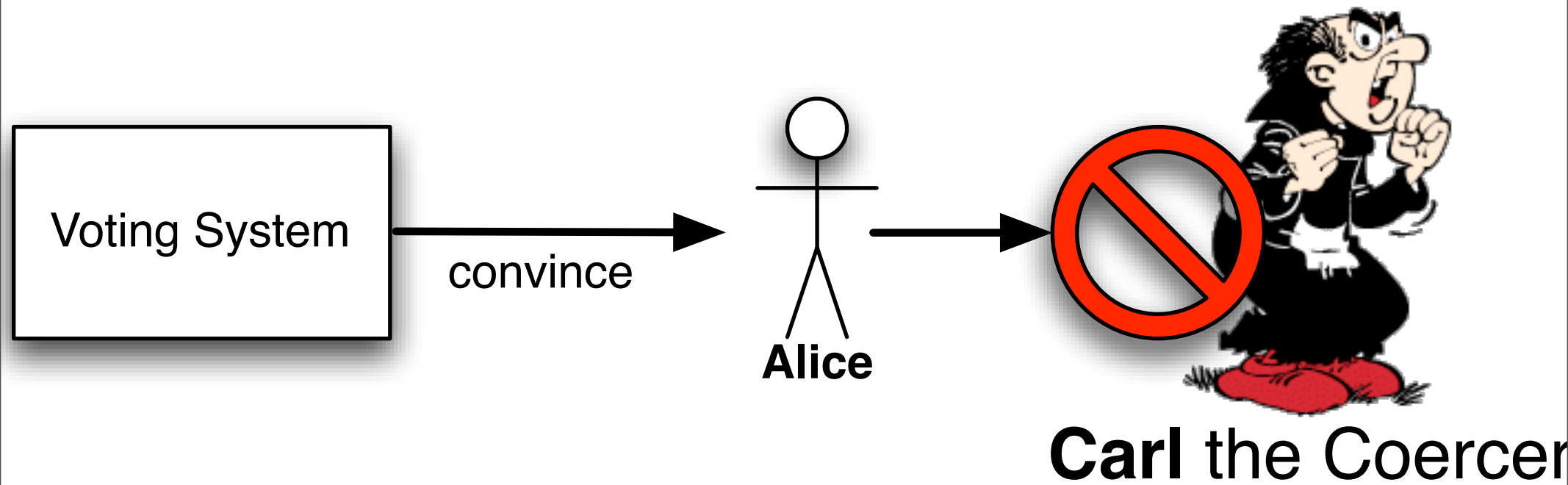


Secret Ballot *vs.* Verifiability



Carl the Coercer

Secret Ballot *vs.* Verifiability



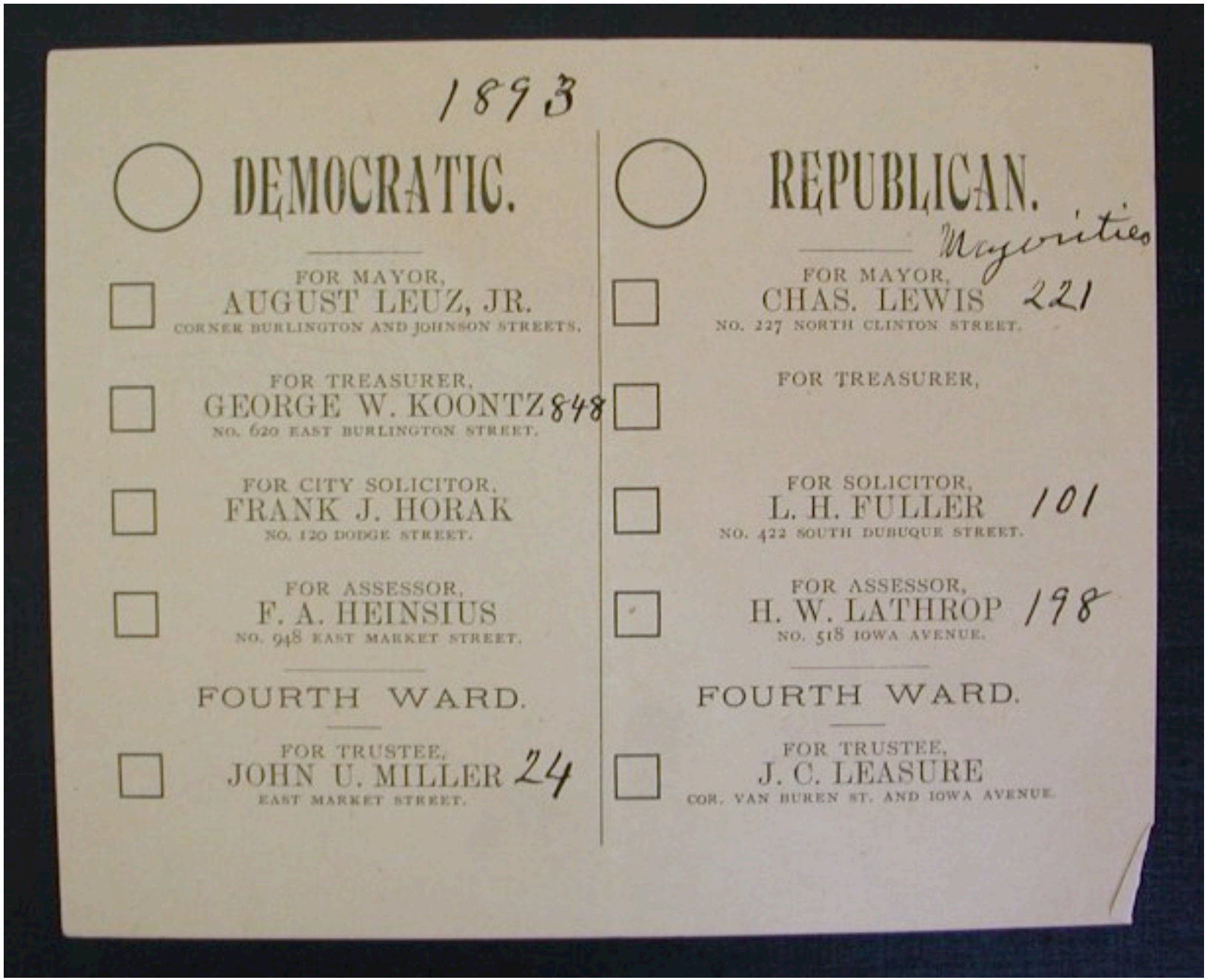
Desired Properties

(1)**Alice** verifies **her vote**.

(2)**Everyone** verifies **tallying**.

(3)Alice **cannot be coerced** by Eve.

1892 - Australian Ballot



1893

DEMOCRATIC.

FOR MAYOR,
AUGUST LEUZ, JR.
CORNER BURLINGTON AND JOHNSON STREETS.

FOR TREASURER,
GEORGE W. KOONTZ 848
NO. 620 EAST BURLINGTON STREET.

FOR CITY SOLICITOR,
FRANK J. HORAK
NO. 120 DODGE STREET.

FOR ASSESSOR,
F. A. HEINSIUS
NO. 948 EAST MARKET STREET.

FOURTH WARD.

FOR TRUSTEE,
JOHN U. MILLER 24
EAST MARKET STREET.

REPUBLICAN.

Majorities

FOR MAYOR,
CHAS. LEWIS 221
NO. 227 NORTH CLINTON STREET.

FOR TREASURER,

FOR SOLICITOR,
L. H. FULLER 101
NO. 422 SOUTH DUBUQUE STREET.

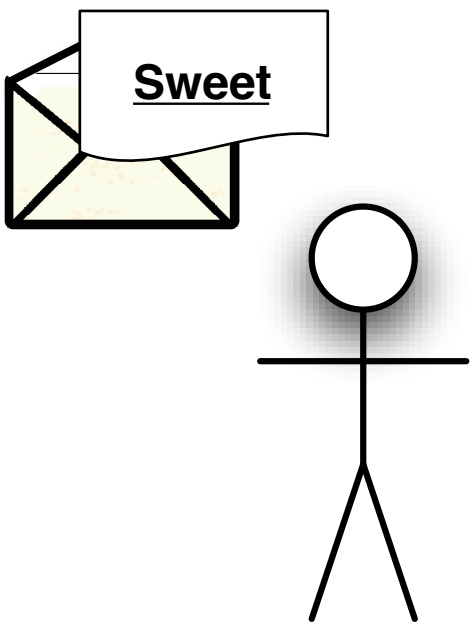
FOR ASSESSOR,
H. W. LATHROP 198
NO. 518 IOWA AVENUE.

FOURTH WARD.

FOR TRUSTEE,
J. C. LEASURE
COR. VAN BUREN ST. AND IOWA AVENUE.

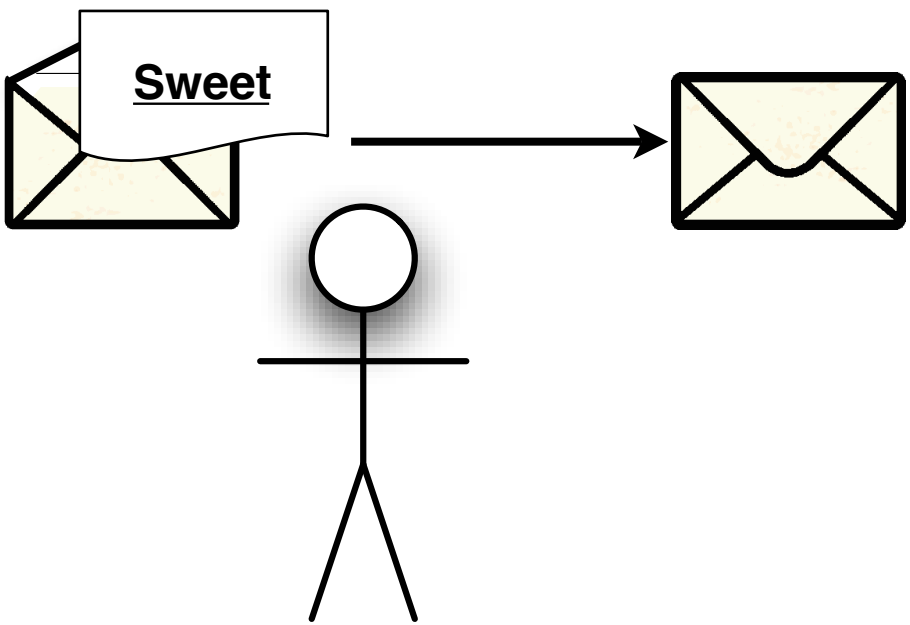
http://www.cs.uiowa.edu/~jones/voting/pictures/

The Ballot Handoff



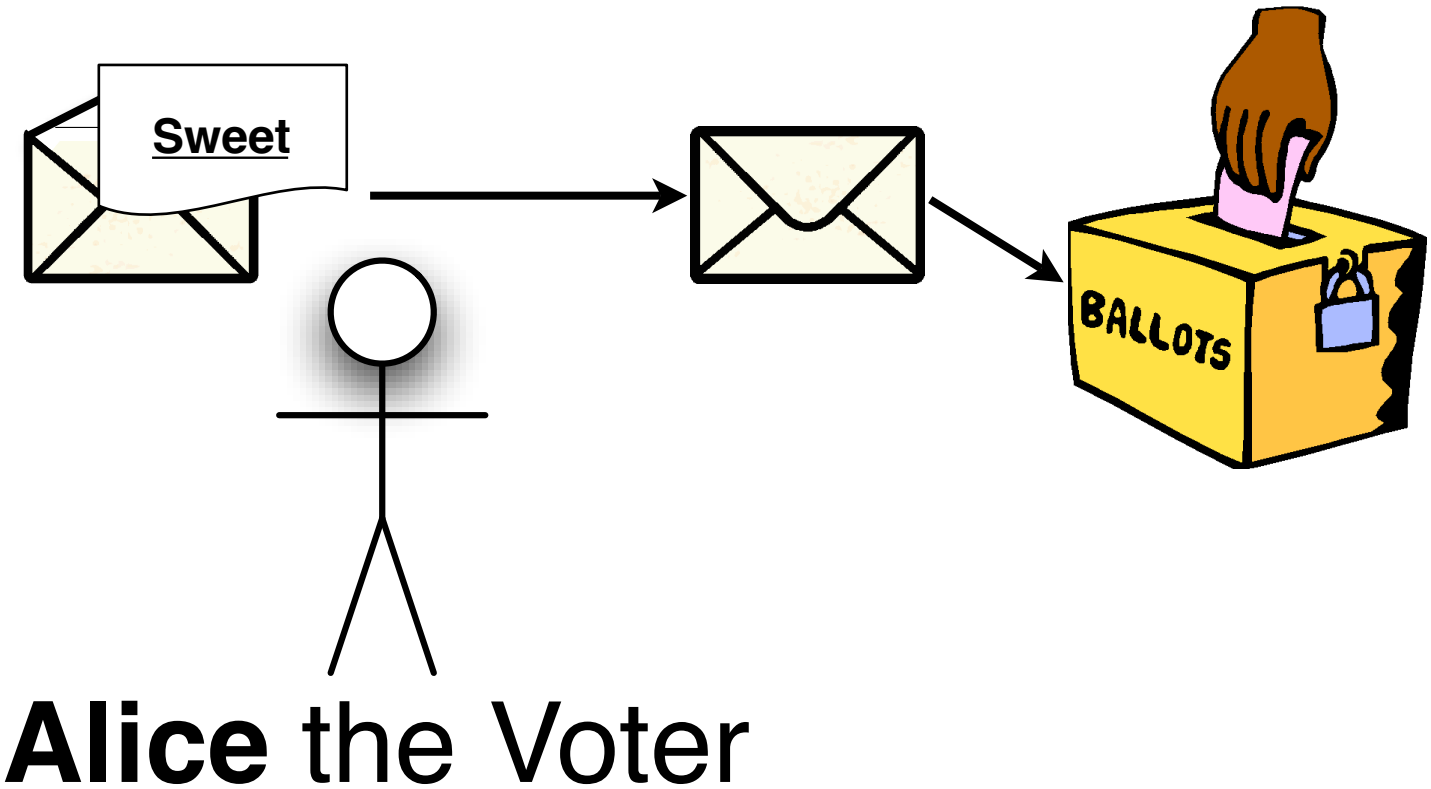
Alice the Voter

The Ballot Handoff

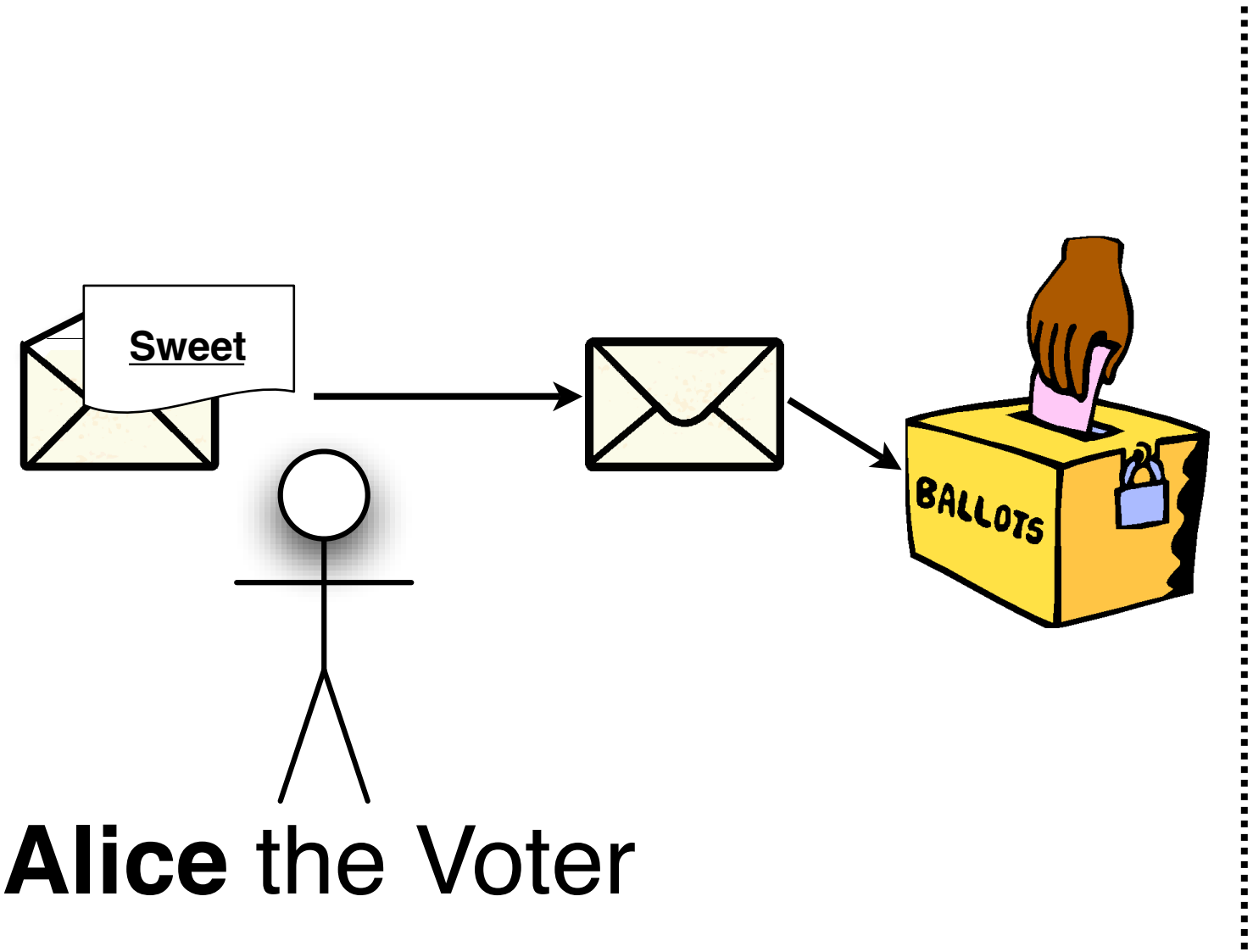


Alice the Voter

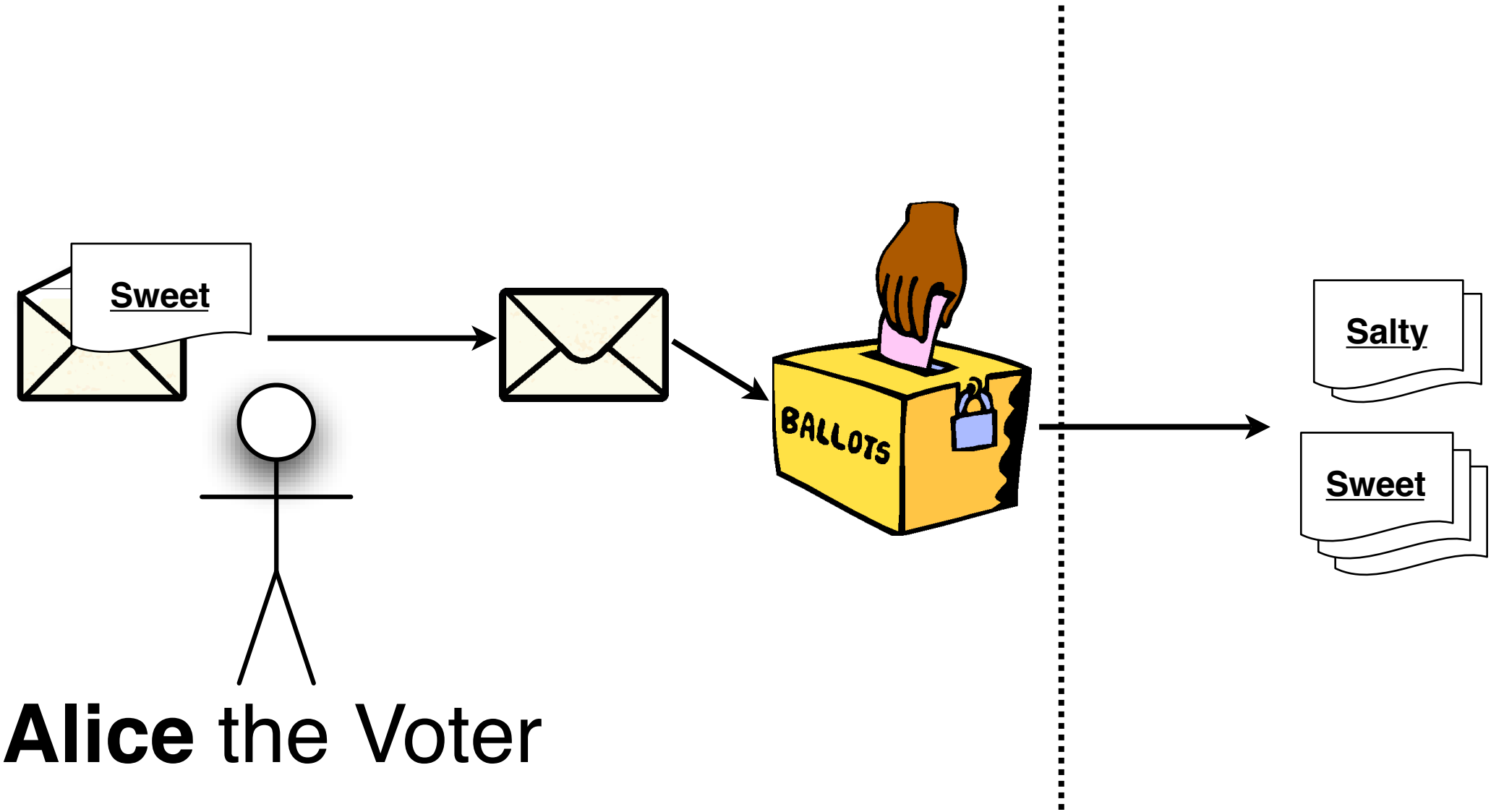
The Ballot Handoff



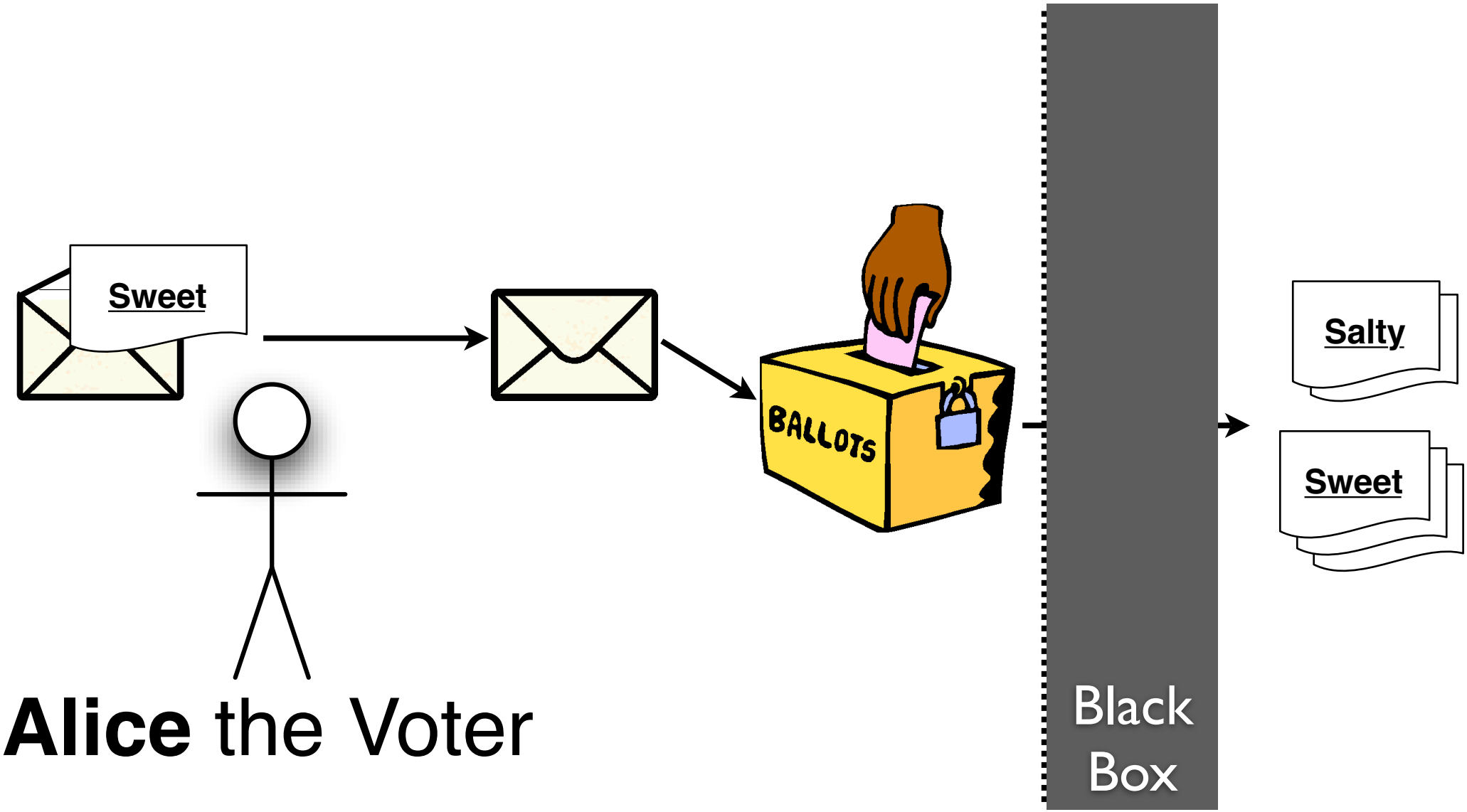
The Ballot Handoff



The Ballot Handoff

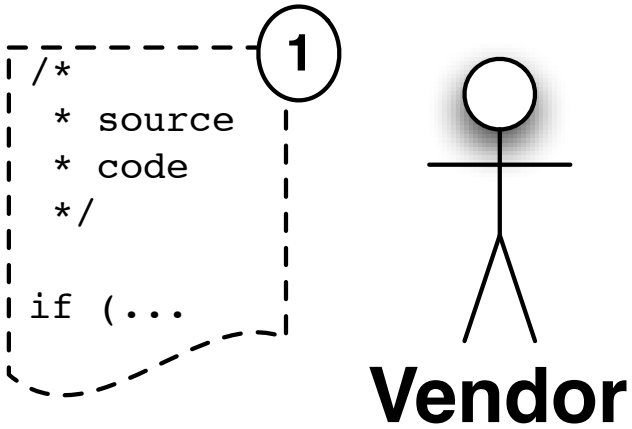


The Ballot Handoff

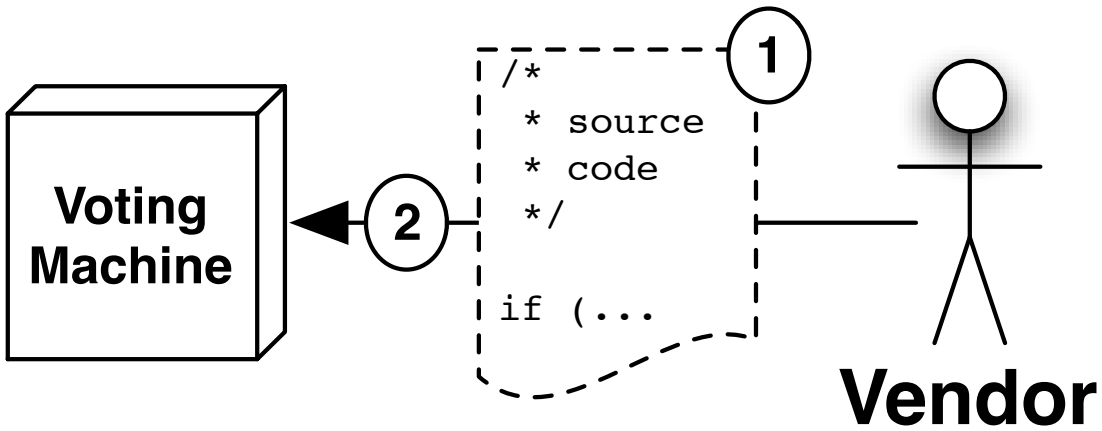


Chain of Custody

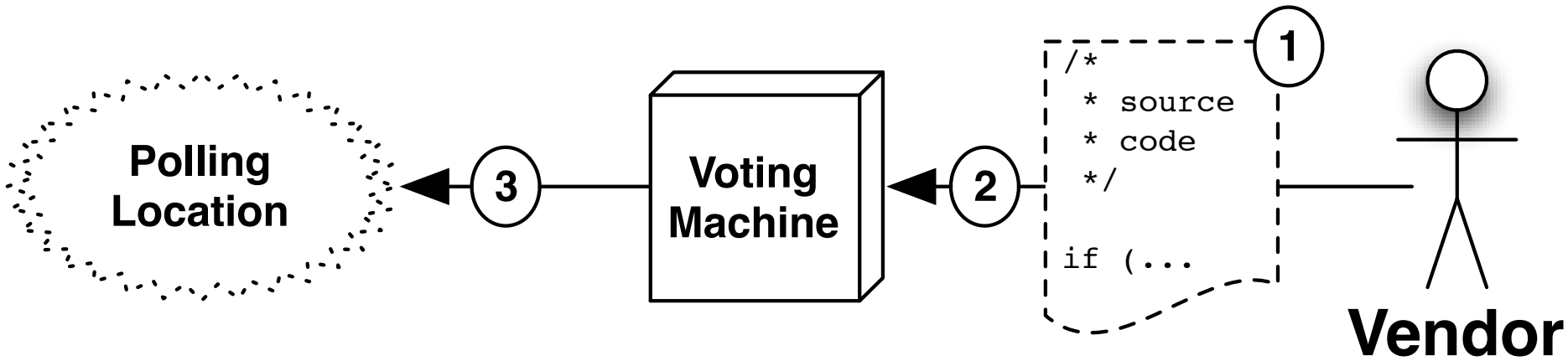
Chain of Custody



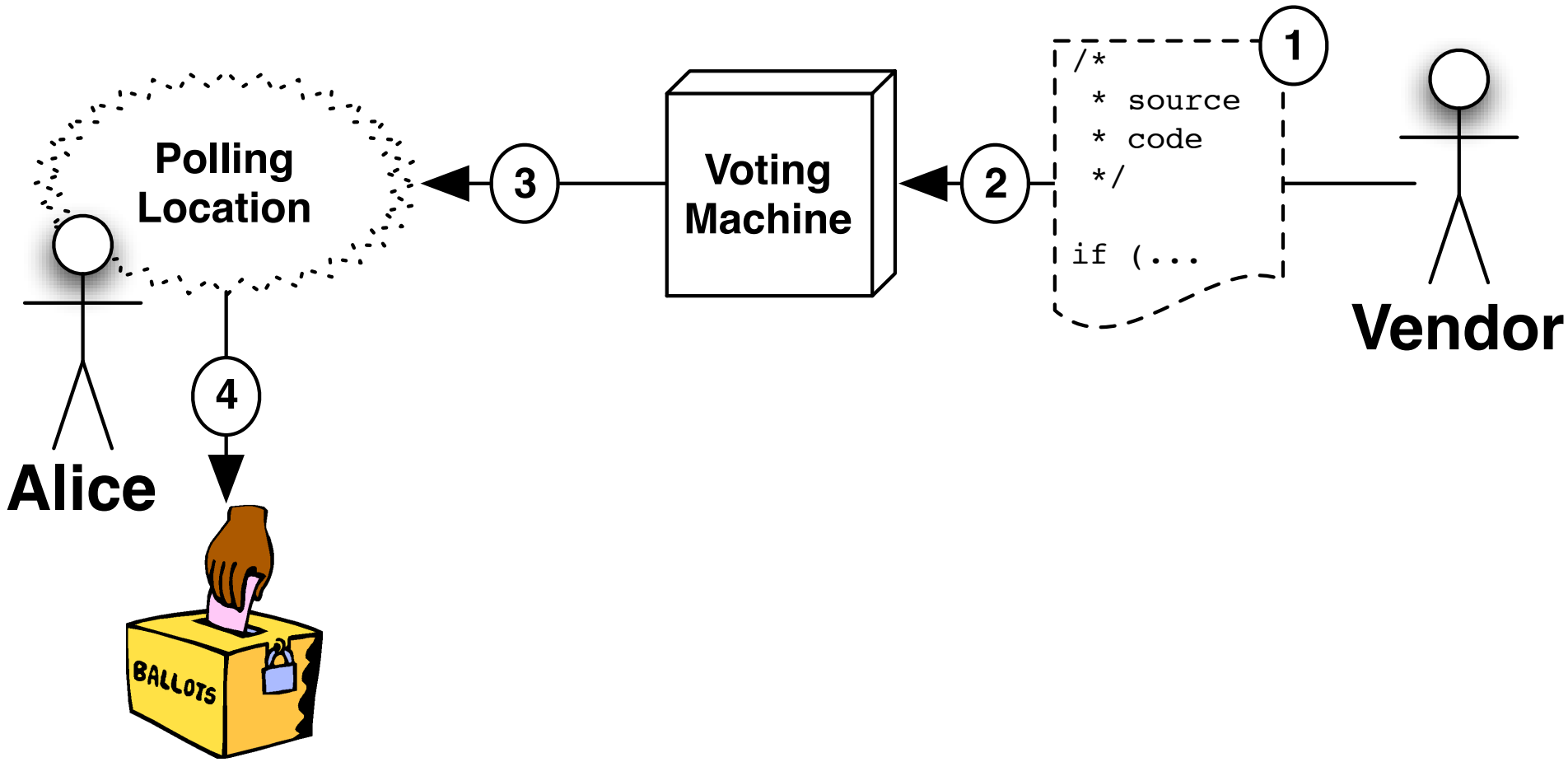
Chain of Custody



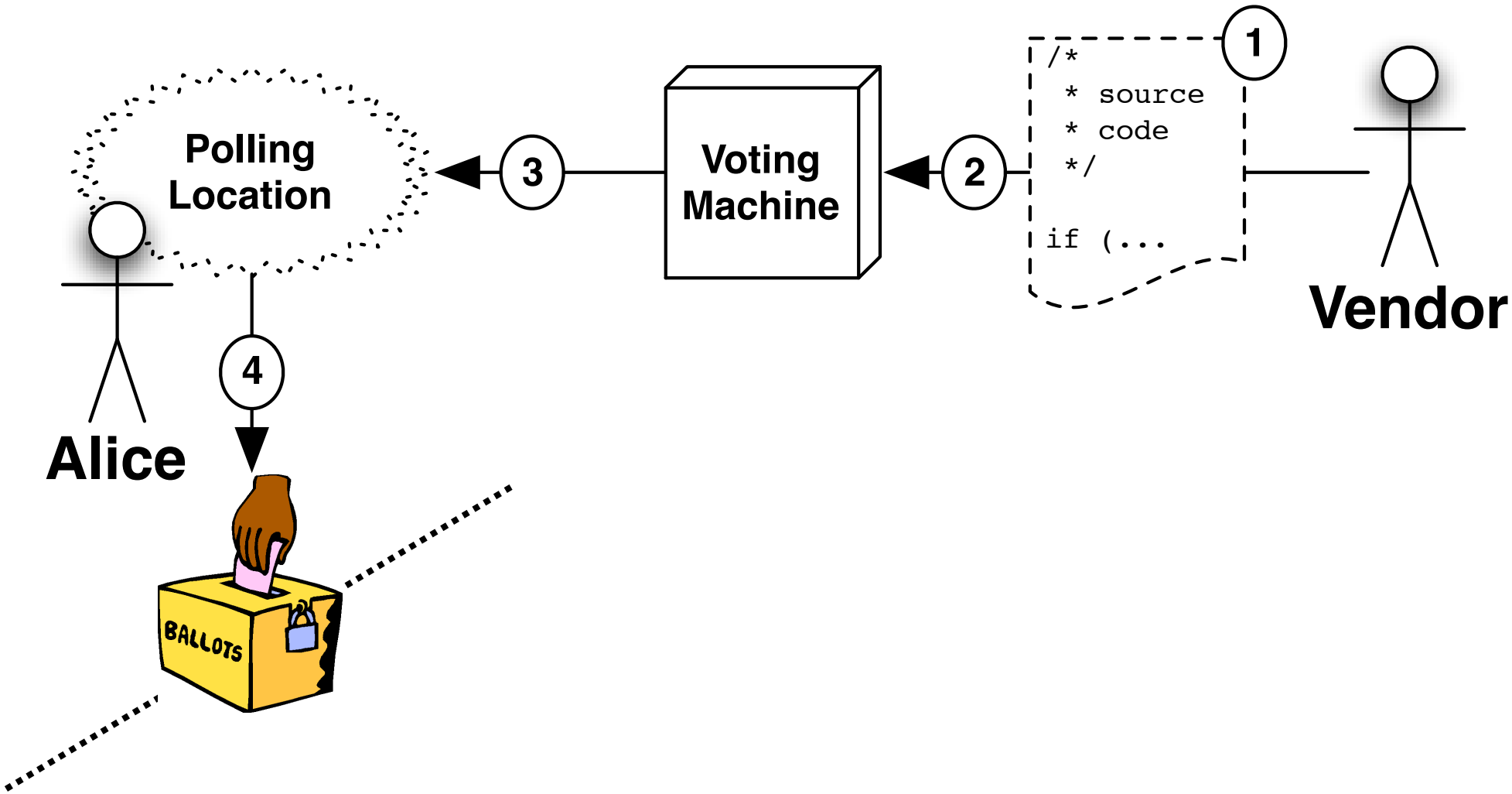
Chain of Custody



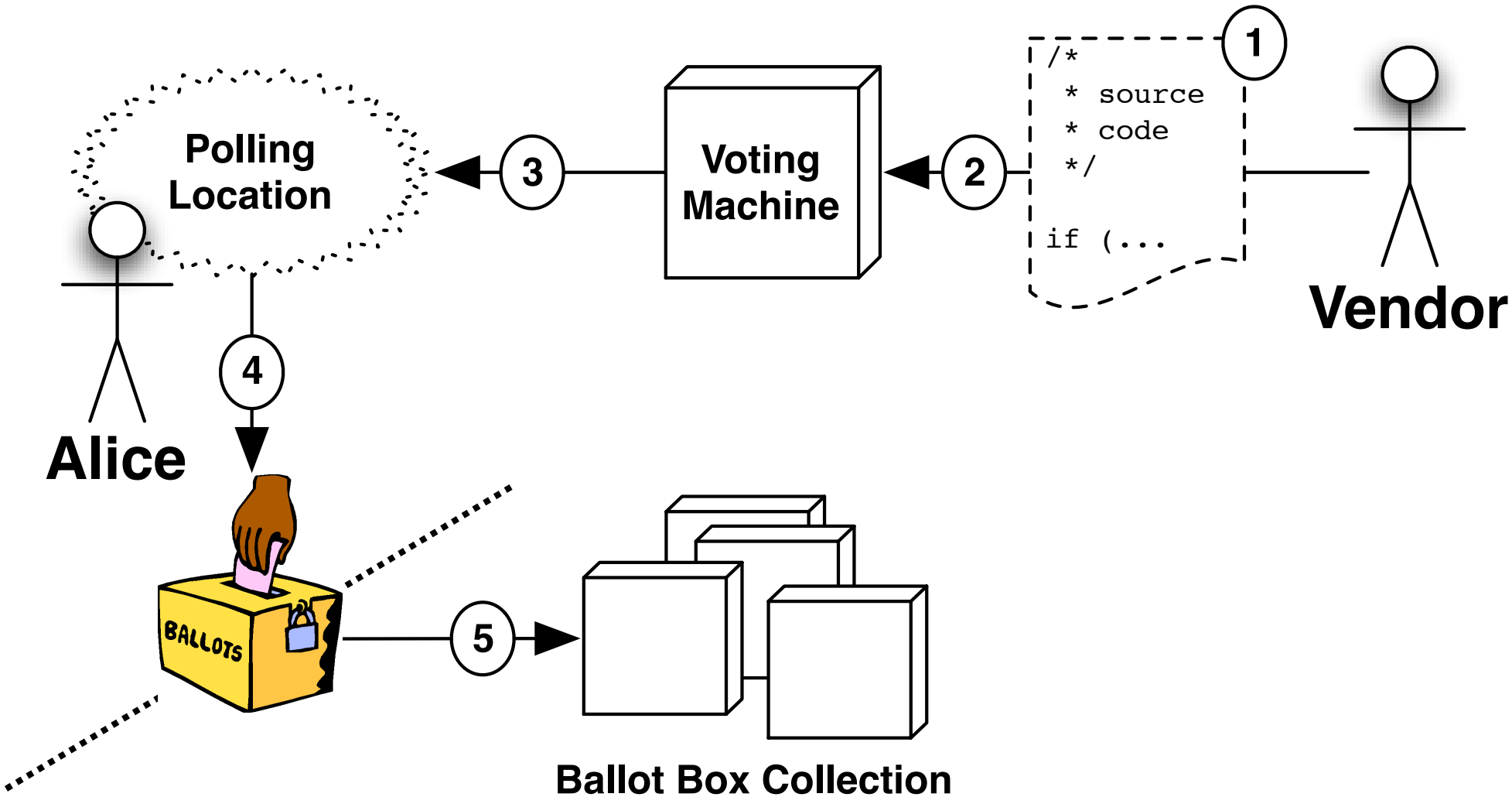
Chain of Custody



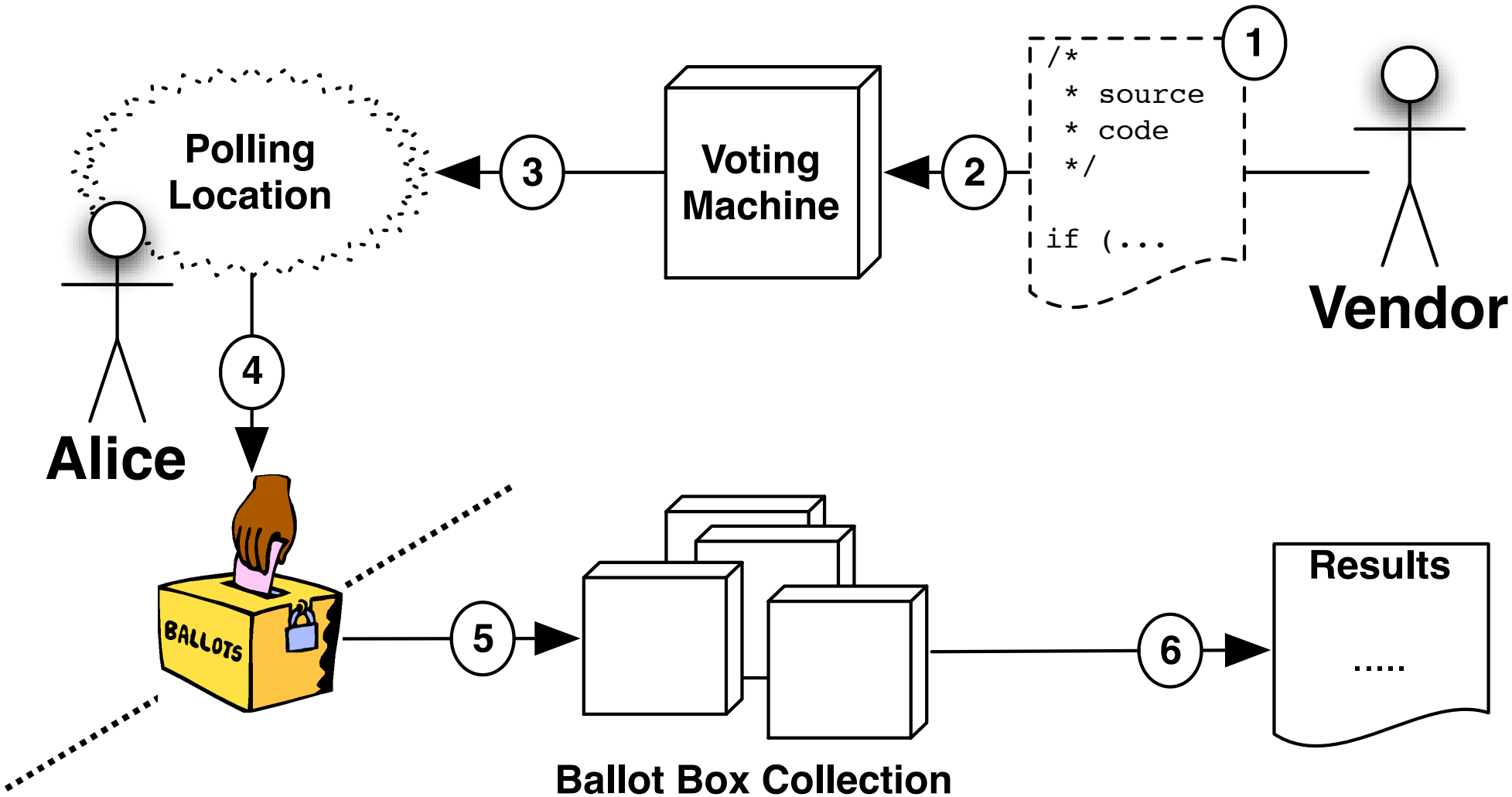
Chain of Custody



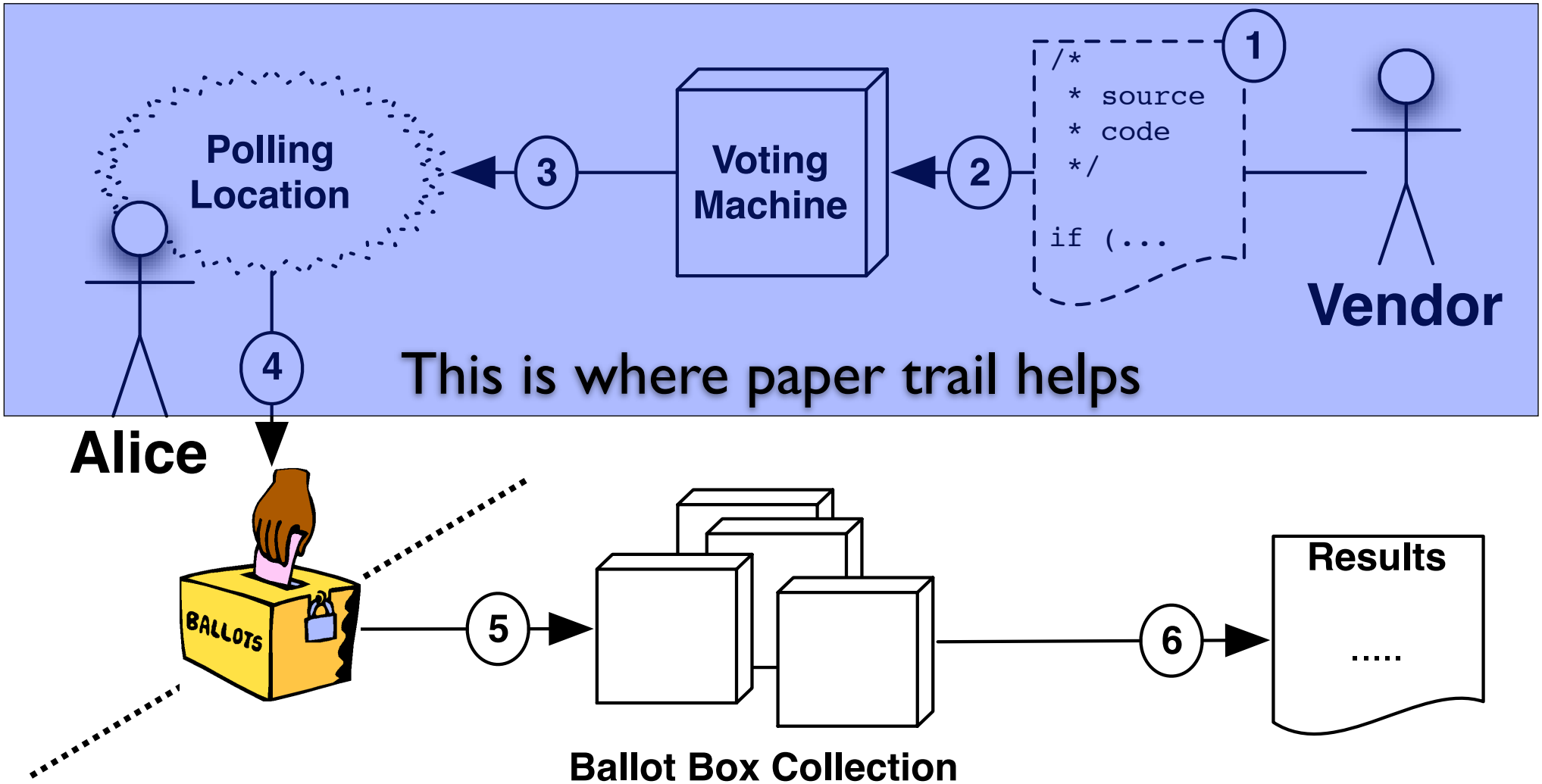
Chain of Custody



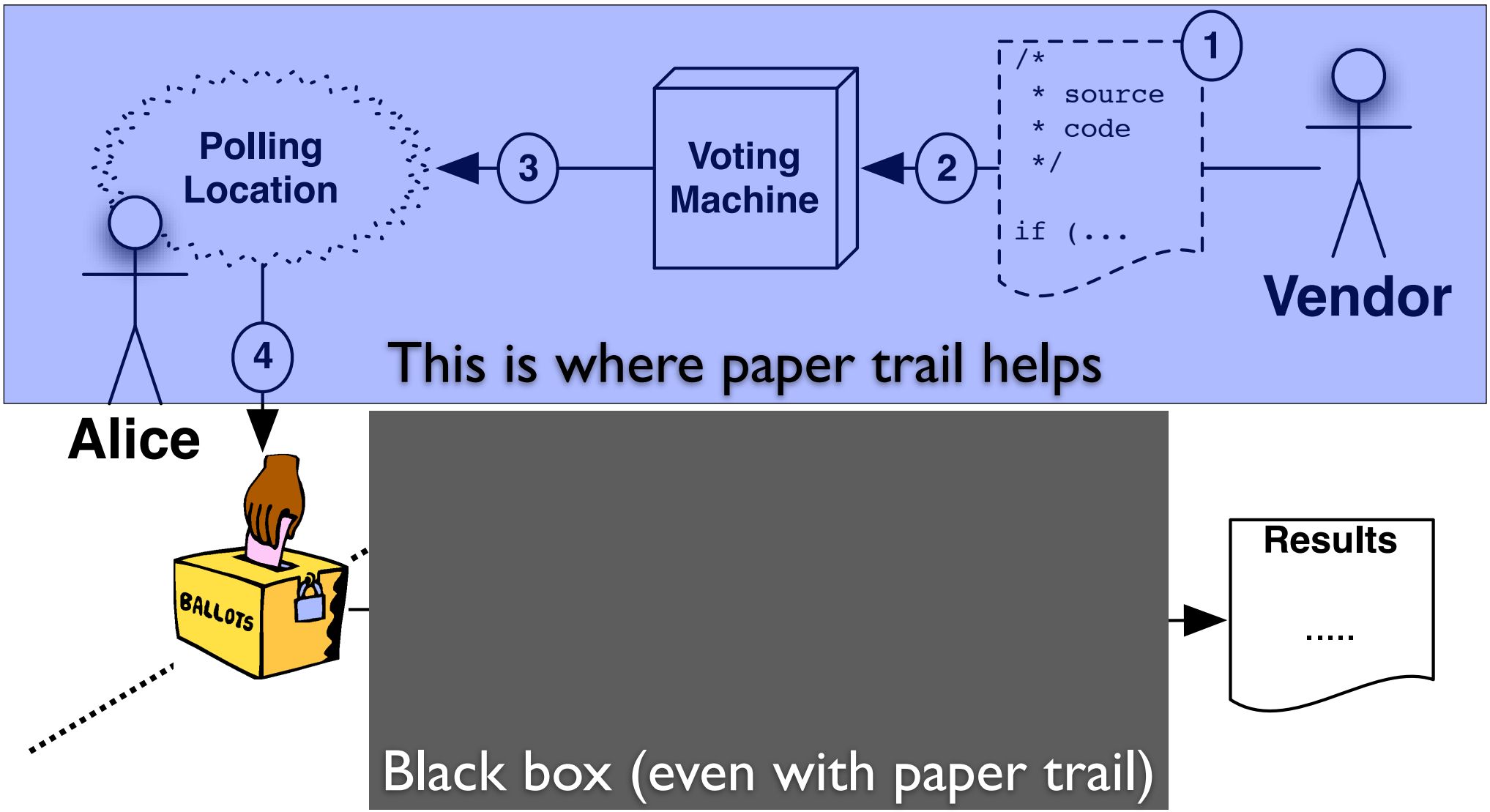
Chain of Custody



Chain of Custody



Chain of Custody



Threat Model

Threat Model

Who is the attacker?

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

How will the attacks be carried out?

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

How will the attacks be carried out?

- ➡ corruption of input, ballot box, transport, tallying

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

How will the attacks be carried out?

- ➡ corruption of input, ballot box, transport, tallying
- ➡ coercion of voters

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

How will the attacks be carried out?

- ➡ corruption of input, ballot box, transport, tallying
- ➡ coercion of voters

Where will the attacks be hidden?

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

How will the attacks be carried out?

- ➡ corruption of input, ballot box, transport, tallying
- ➡ coercion of voters

Where will the attacks be hidden?

- ➡ honest mistakes: randomly distributed in the process

Threat Model

Who is the attacker?

- ➡ administration officials, candidates, poll workers, even voters

What is the Benefit?

How will the attacks be carried out?

- ➡ corruption of input, ballot box, transport, tallying
- ➡ coercion of voters

Where will the attacks be hidden?

- ➡ honest mistakes: randomly distributed in the process
- ➡ malicious intent: hiding where you least defend

So what can we do?

Wooten got the news from his wife, Roxanne, who went to City Hall on Wednesday to see the election results.

"She saw my name with *zero* votes by it. She came home and asked me if I had voted for myself or not. I told her I did," said Wooten, owner of local bar.

Open audit elections

Cryptography provides more than confidentiality.

Cryptography can provide both **verifiability** *and* **ballot secrecy**

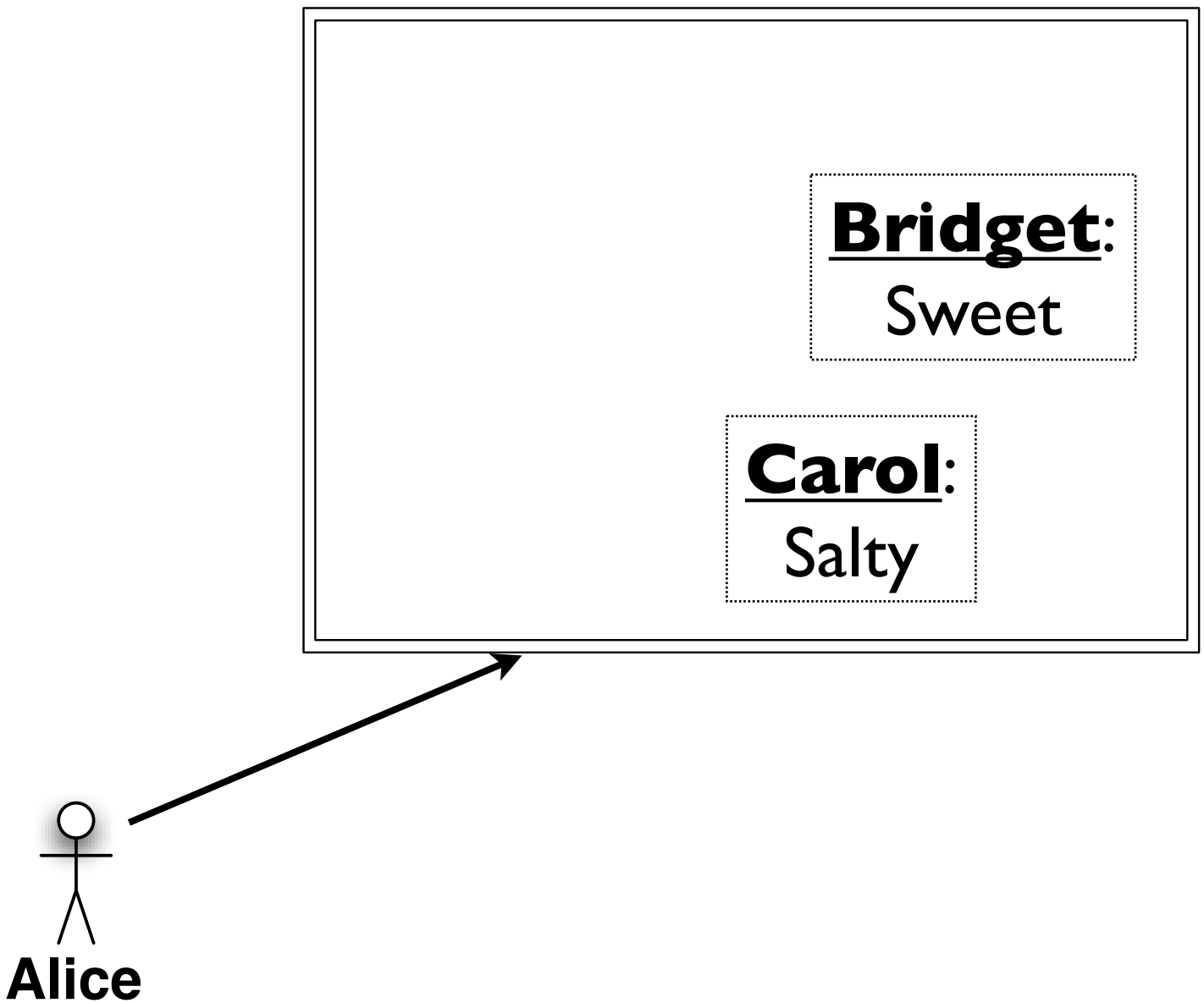
Anyone can audit!

Public Ballots

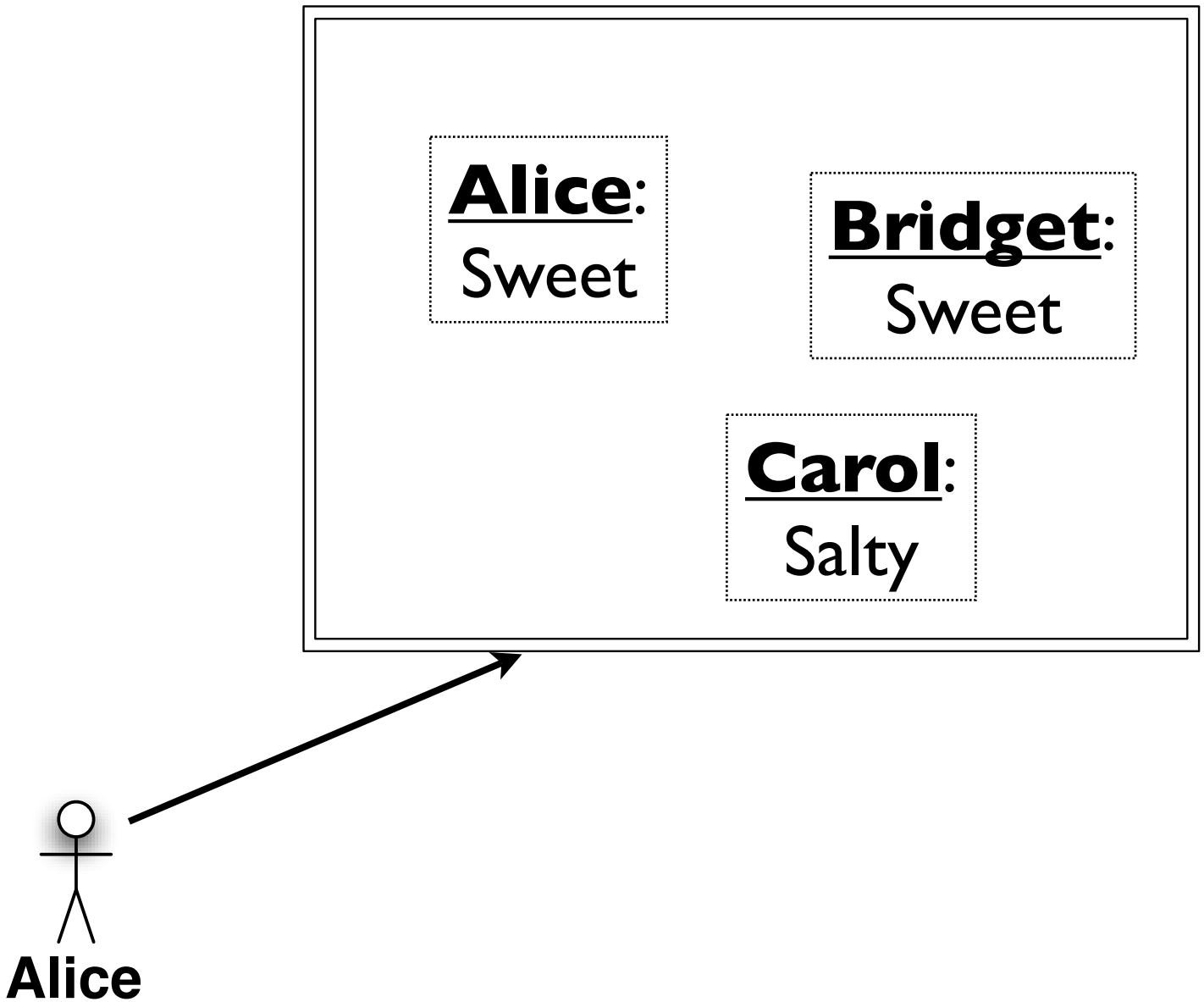
Bridget:
Sweet

Carol:
Salty

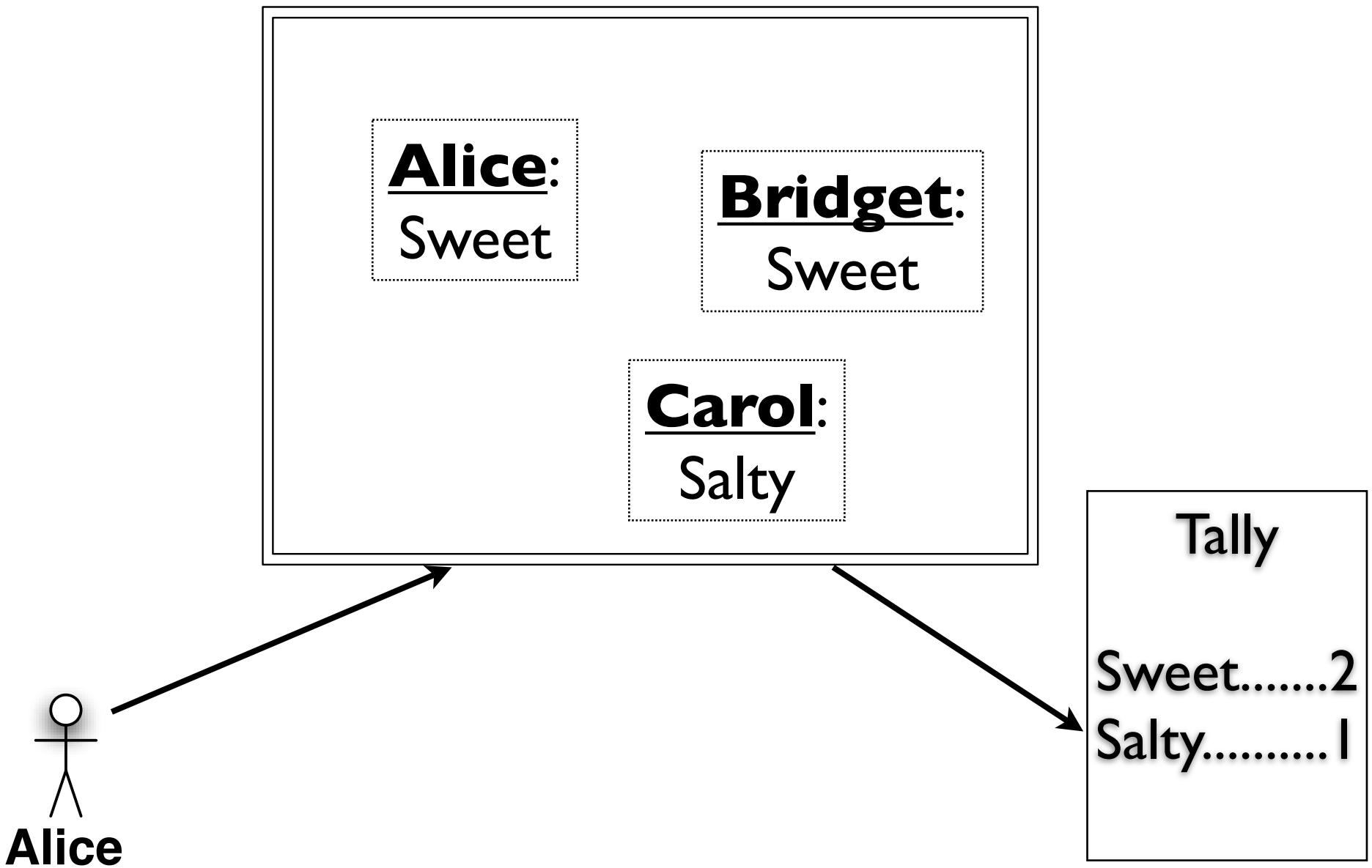
Public Ballots



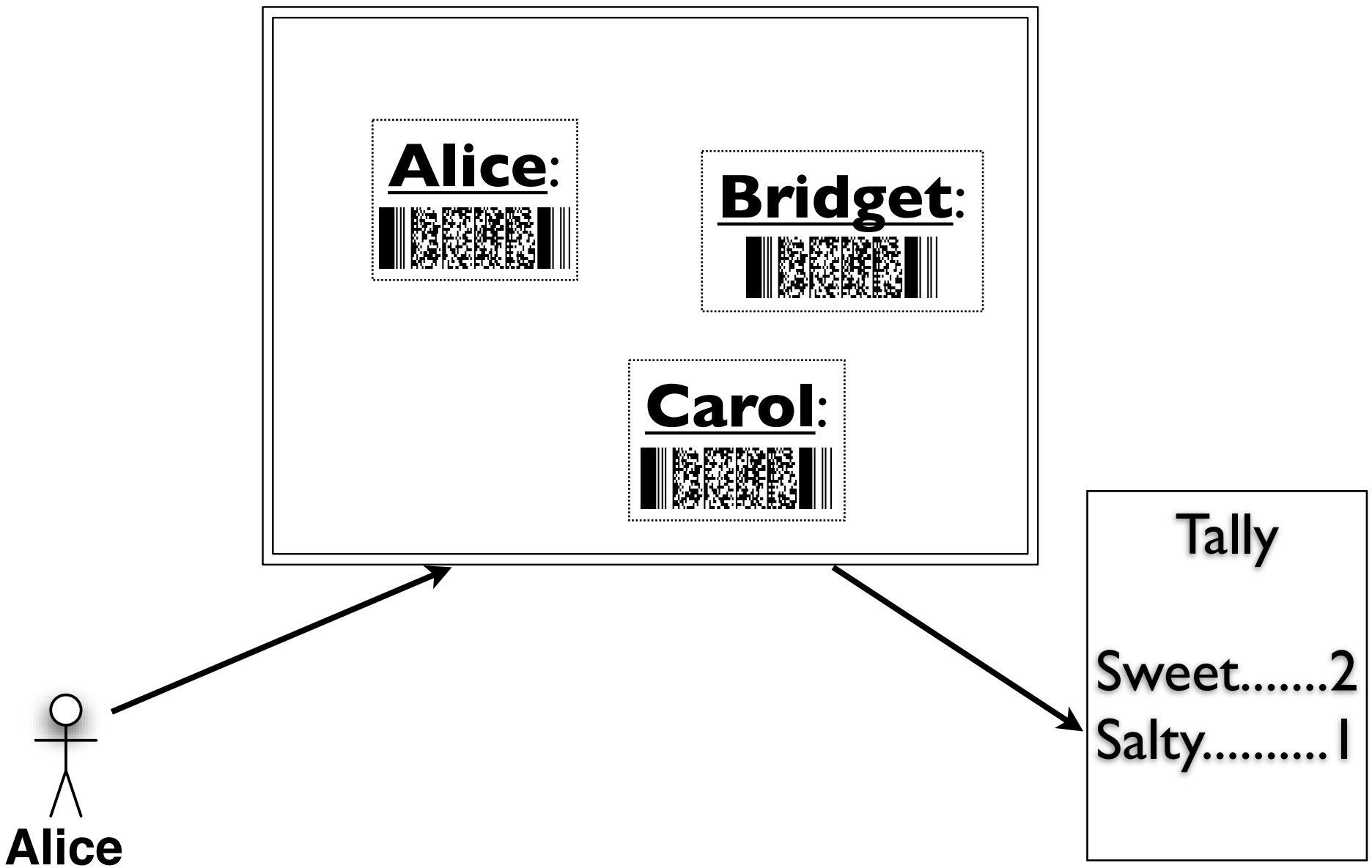
Public Ballots



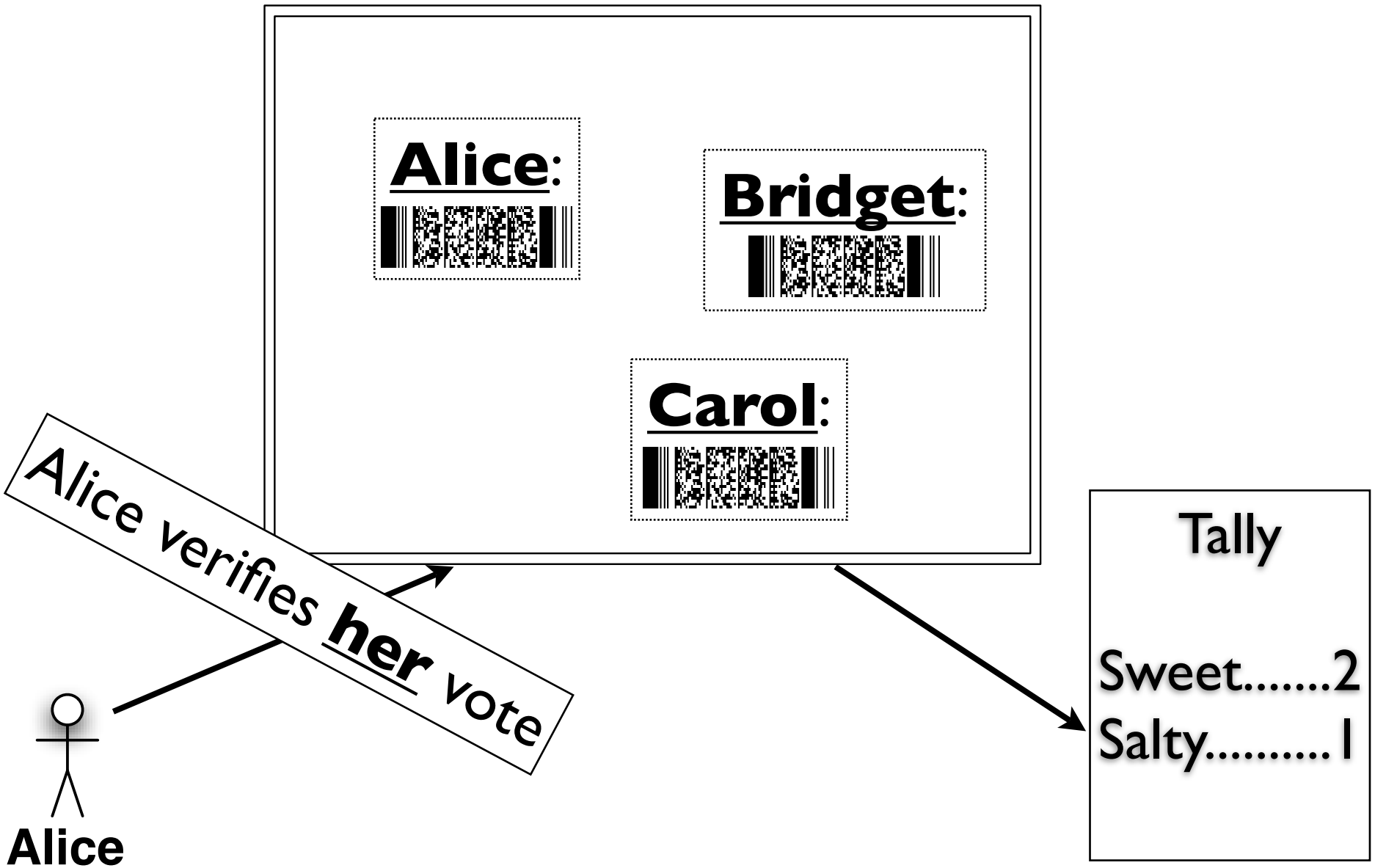
Public Ballots



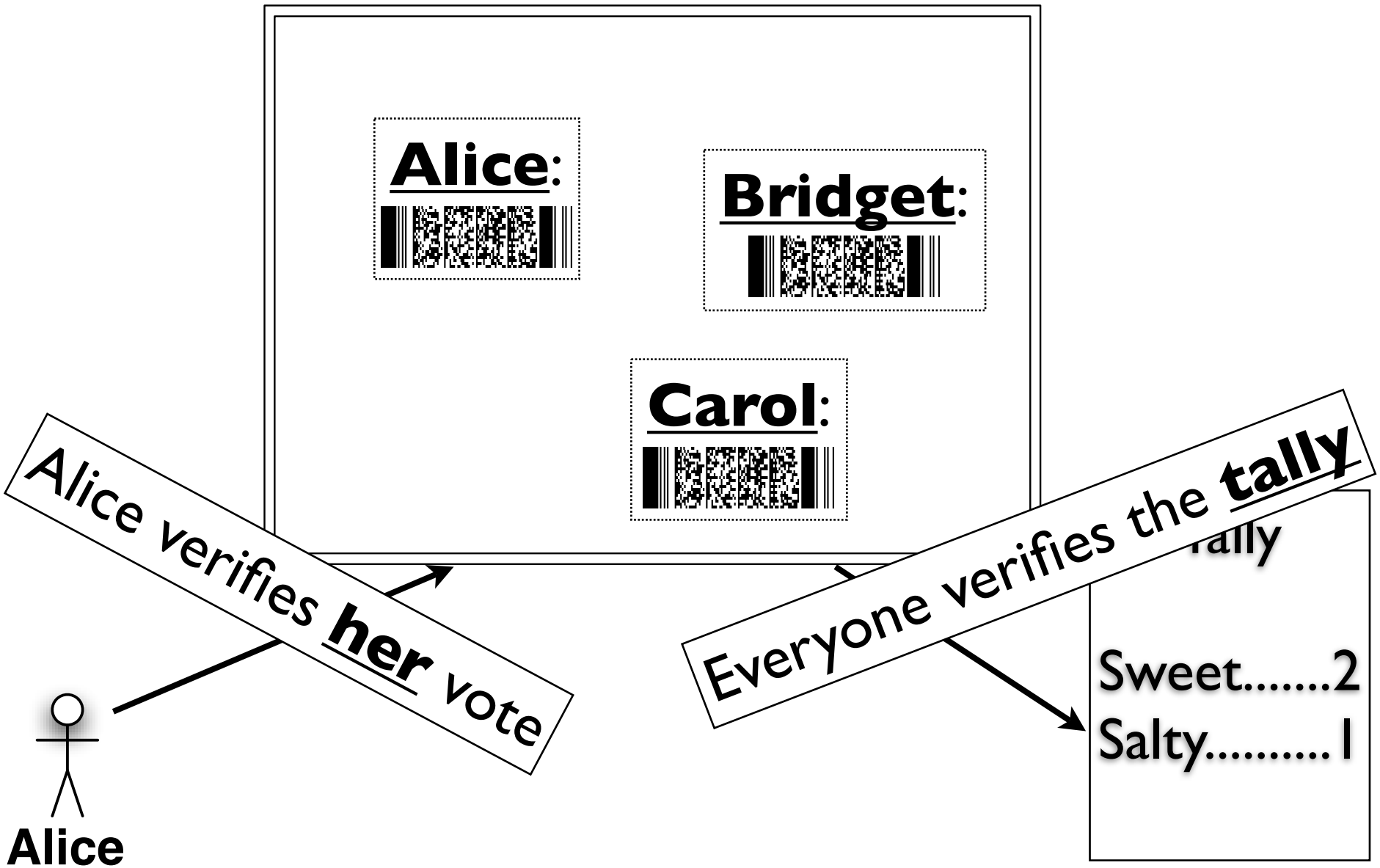
Encrypted Public Ballots



Encrypted Public Ballots



Encrypted Public Ballots



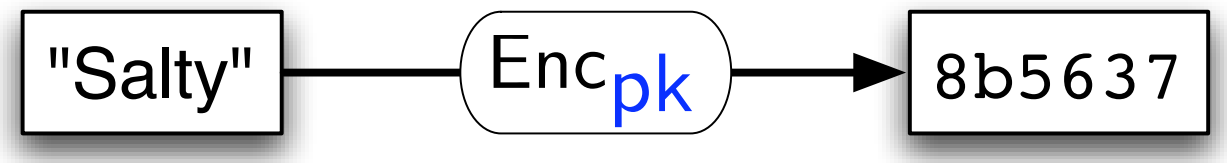
Public-Key Encryption

Public-Key Encryption

Keypair consists of a public key pk and a secret key sk.

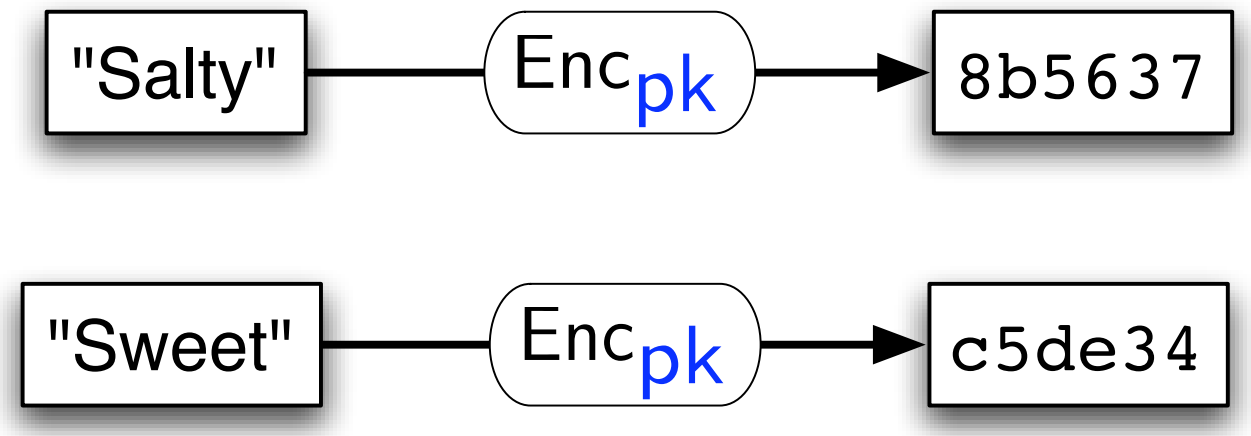
Public-Key Encryption

Keypair consists of a public key pk and a secret key sk.



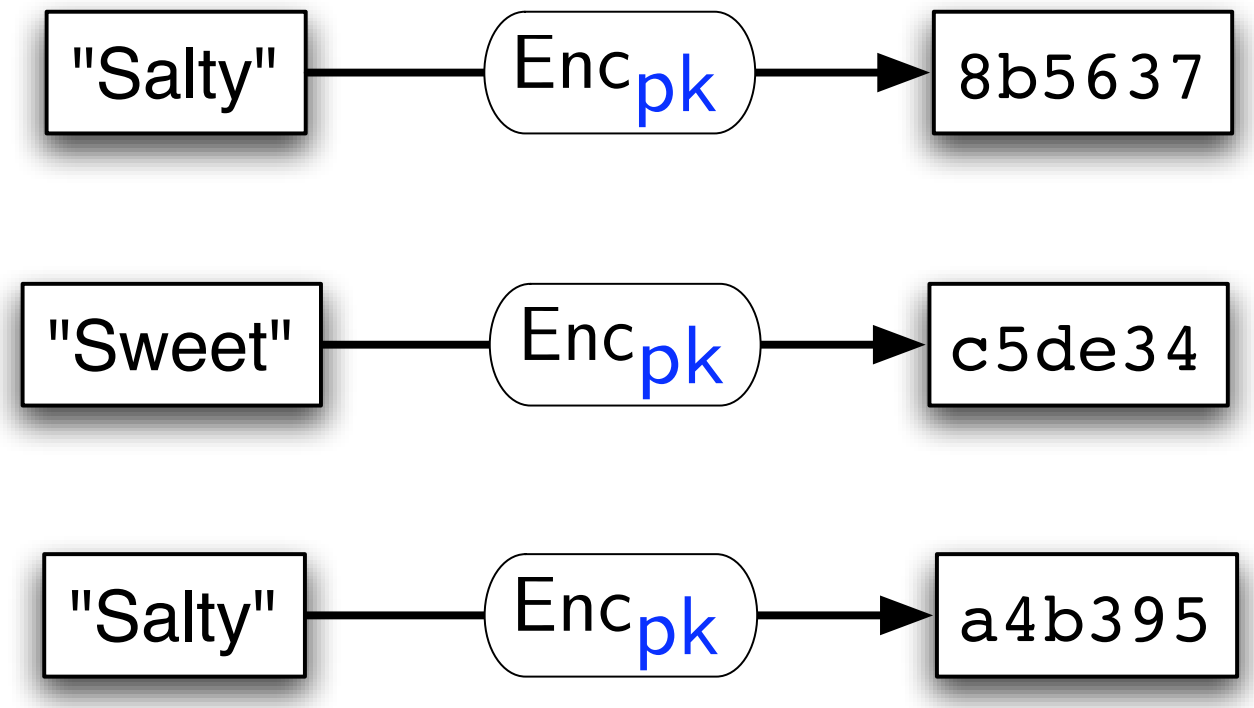
Public-Key Encryption

Keypair consists of a public key pk and a secret key sk.



Public-Key Encryption

Keypair consists of a public key pk and a secret key sk.



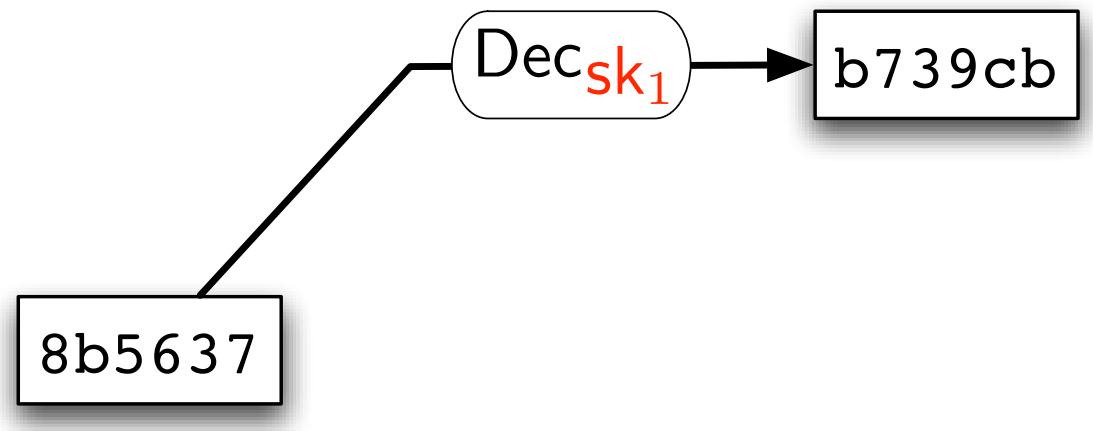
Threshold Decryption

Secret key is shared amongst multiple parties:
all (or at least a quorum) need to cooperate to decrypt.

8b5637

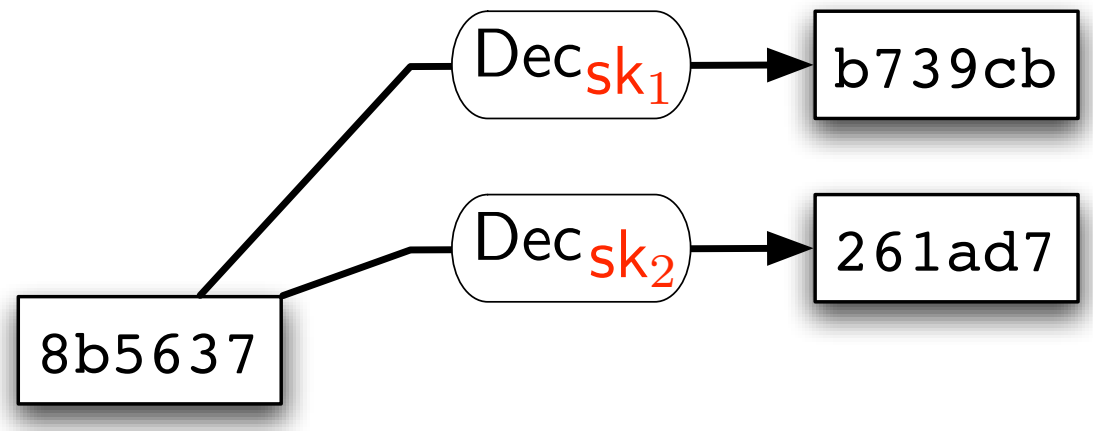
Threshold Decryption

Secret key is shared amongst multiple parties:
all (or at least a quorum) need to cooperate to decrypt.



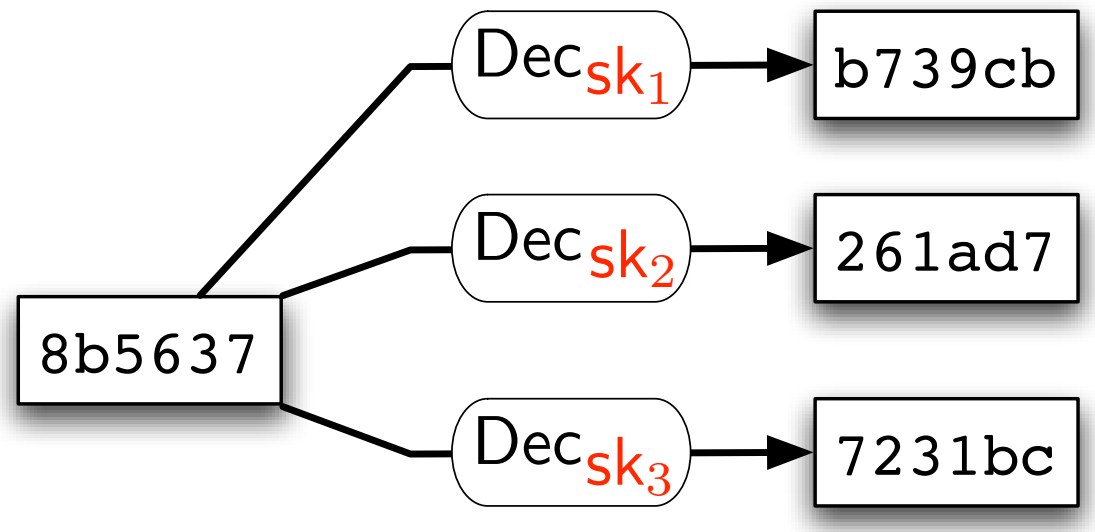
Threshold Decryption

Secret key is shared amongst multiple parties:
all (or at least a quorum) need to cooperate to decrypt.



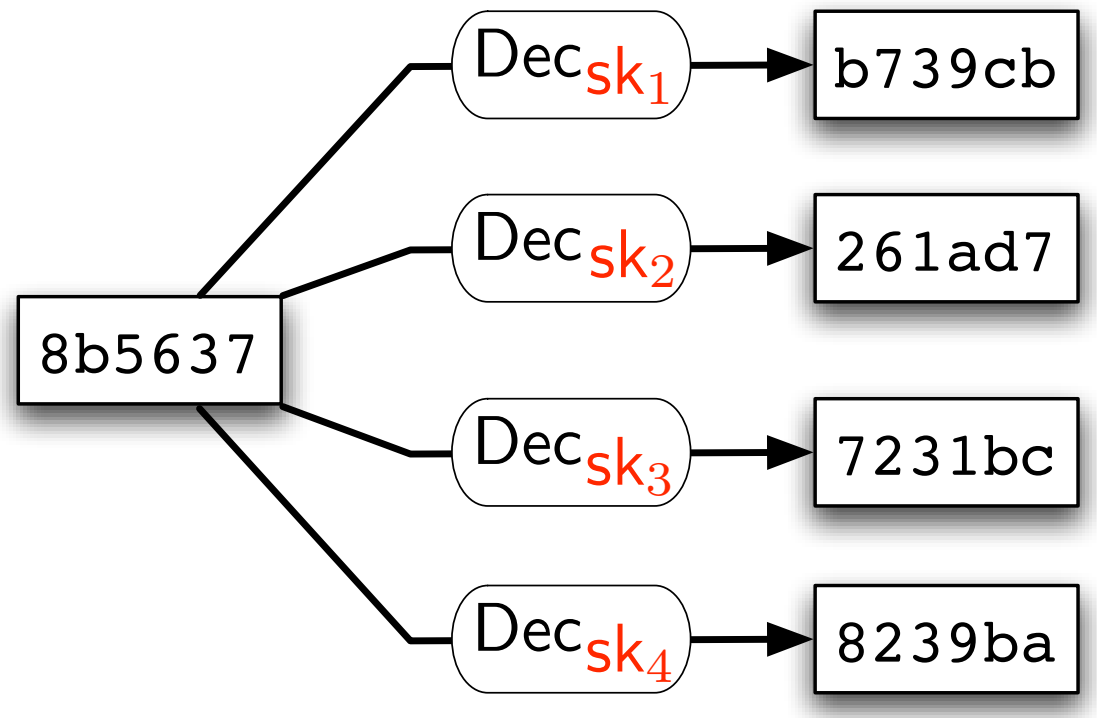
Threshold Decryption

Secret key is shared amongst multiple parties:
all (or at least a quorum) need to cooperate to decrypt.



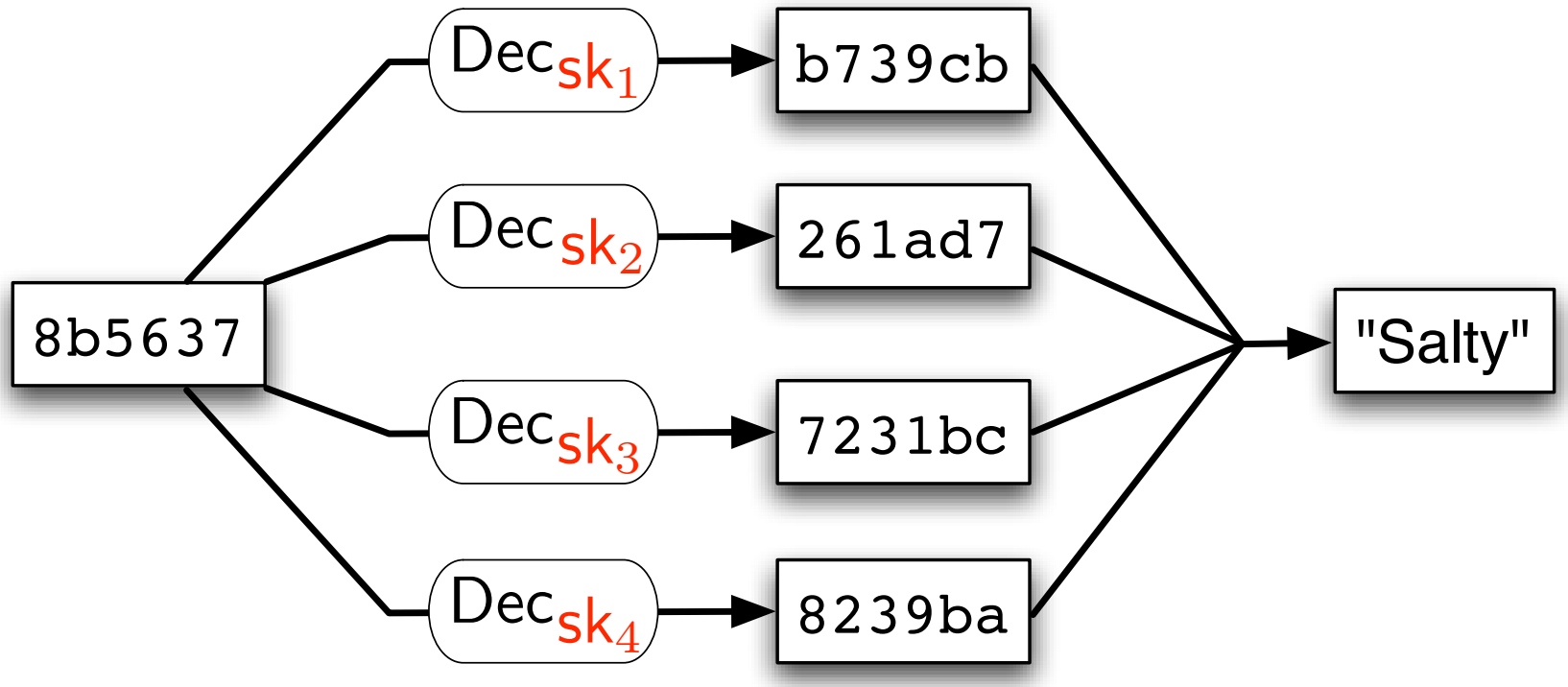
Threshold Decryption

Secret key is shared amongst multiple parties:
all (or at least a quorum) need to cooperate to decrypt.



Threshold Decryption

Secret key is shared amongst multiple parties:
all (or at least a quorum) need to cooperate to decrypt.



Tallying Method I: Homomorphic Tabulation [Benaloh'87]

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

Tallying Method I: Homomorphic Tabulation [Benaloh'87]

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

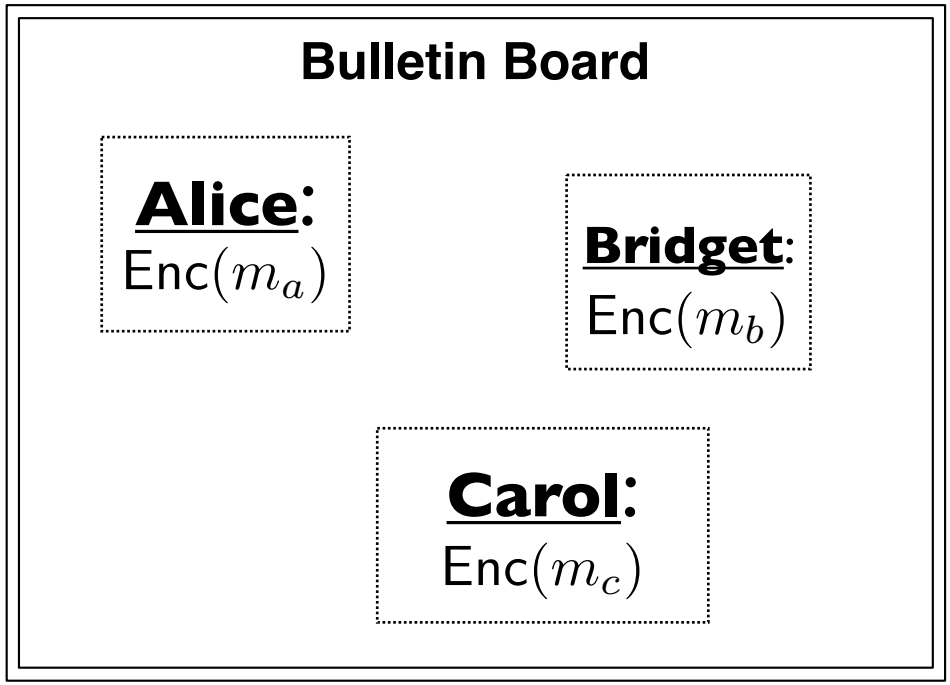
$$\mathsf{Yes} = \mathsf{Enc}(1)$$
$$\mathsf{No} = \mathsf{Enc}(0)$$

Tallying Method I: Homomorphic Tabulation [Benaloh'87]

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

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

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

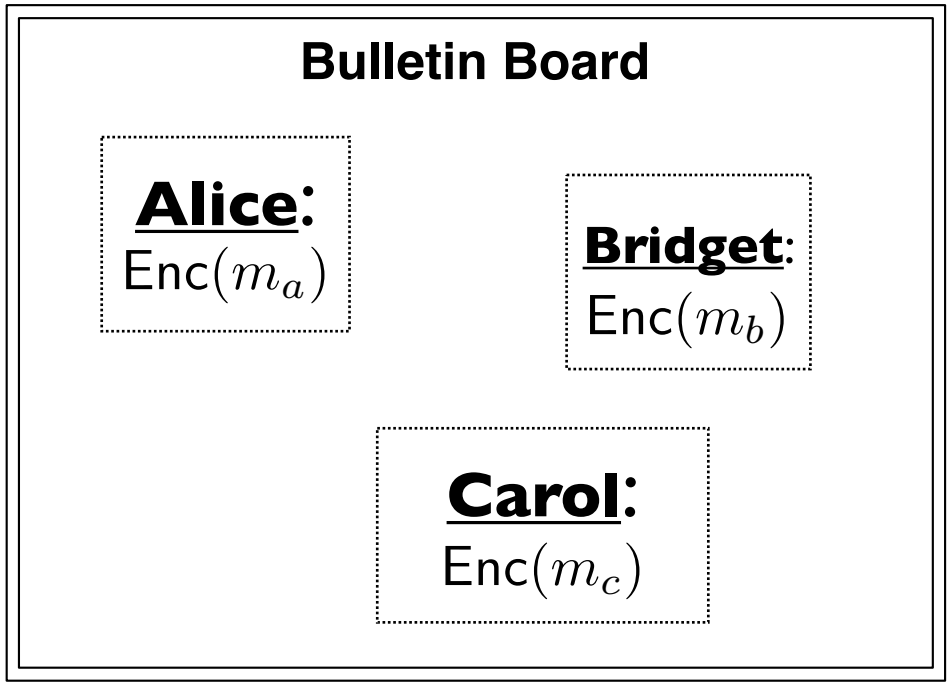


Tallying Method I: Homomorphic Tabulation [Benaloh'87]

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

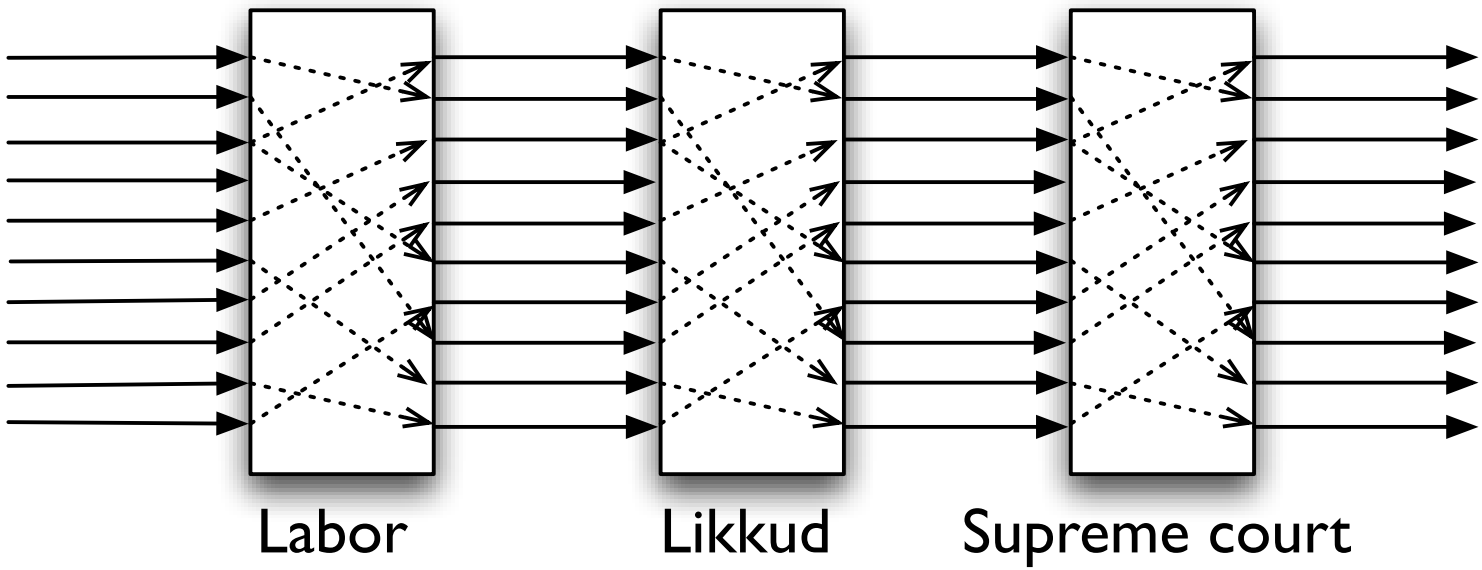
$$\mathsf{Yes} = \mathsf{Enc}(1)$$

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

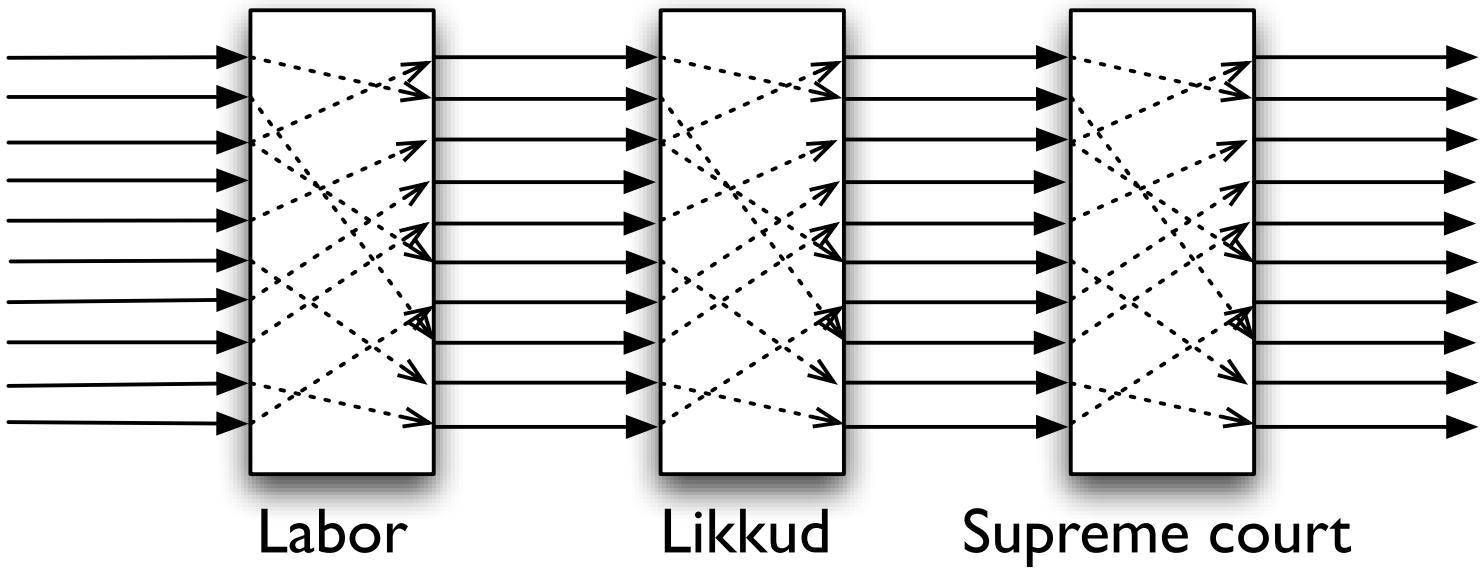


$$\mathsf{EncryptedTally} = \mathsf{Enc}(m_a) \times \mathsf{Enc}(m_b) \times \mathsf{Enc}(m_c) = \mathsf{Enc}(m_a + m_b + m_c)$$

Tallying Method II: Mixnet [Chaum'81]



Tallying Method II: Mixnet [Chaum'81]



Each mix server shuffles the encrypted votes.

How can we **verify** operations on **encrypted** data?

Verifying Validity of Encryption/Mixing

Given Enc(*m*) How can I verify:

1. that it is not an encryption of more than one vote?
2. that the encryption of my vote wasn't "dropped"?

<u>Zero-Knowledge proofs</u>: Can prove validity of Enc(*m*) without revealing anything else!

<u>The crucial point</u>: only need to verify that machine is computing right functionality...

Verifying Validity of Encryption/Mixing

Given Enc(*m*) How can I verify:

1. that it is not an encryption of more than one vote?
2. that the encryption of my vote wasn't "dropped"?

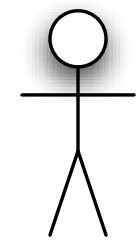
<u>Zero-Knowledge proofs</u>: Can prove validity of Enc(*m*) without revealing anything else!

<u>The crucial point</u>: only need to verify that machine is computing right functionality...

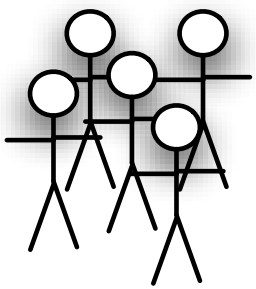
Voting Process Example

[Chaum'81, Sako-Kilian'95, Neff'04, Chaum'04, etc...]

Identification

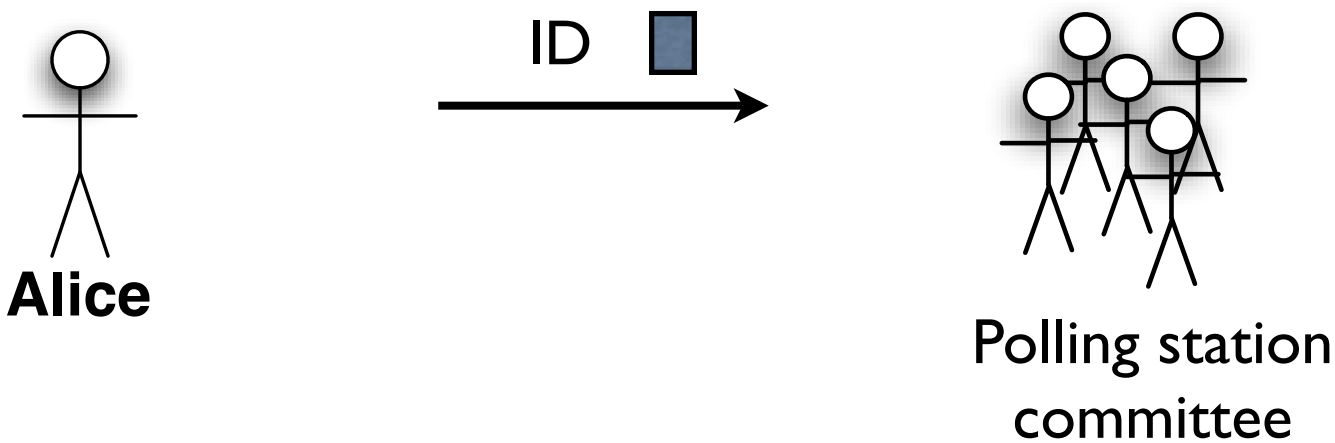


Alice

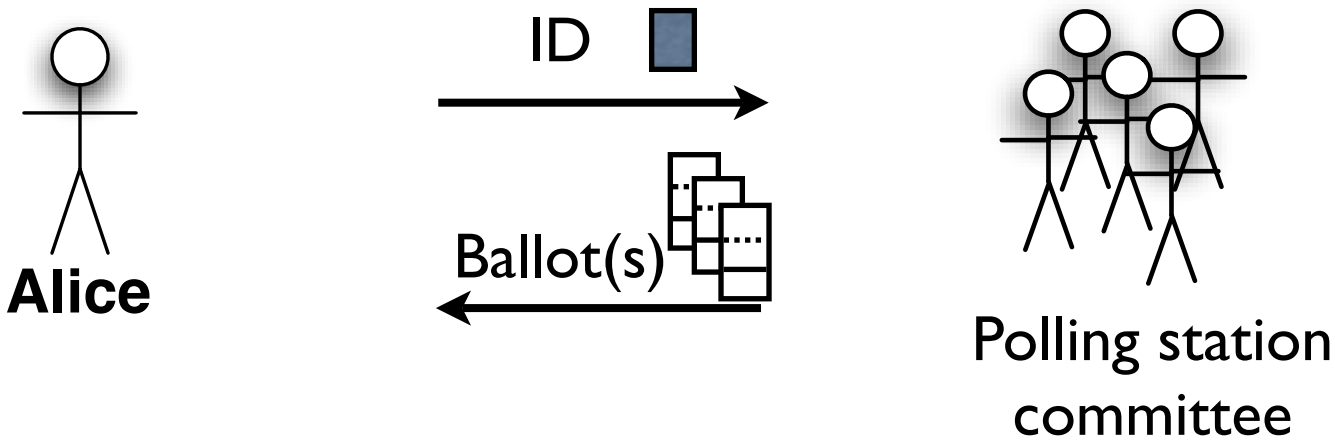


Polling station committee

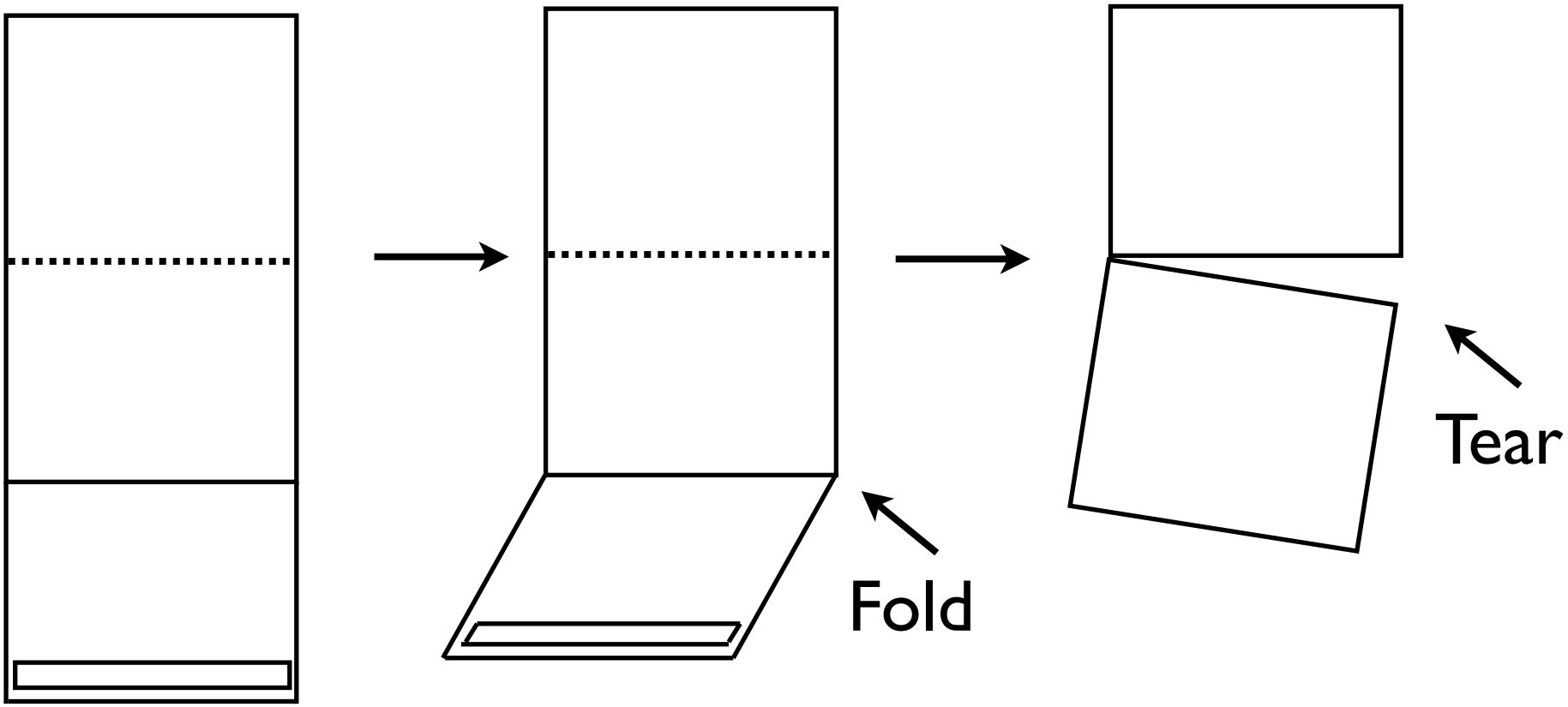
Identification



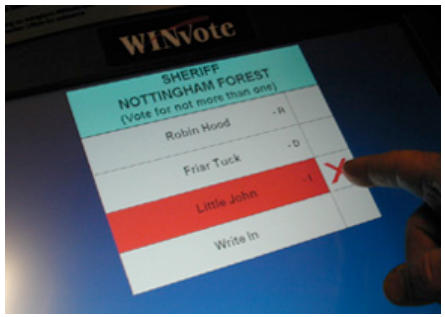
Identification



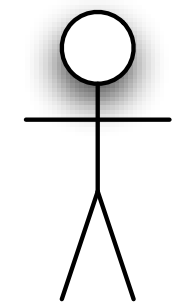
The Ballot



Producing Encrypted Ballot

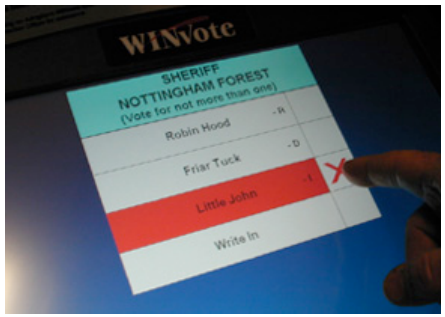


+

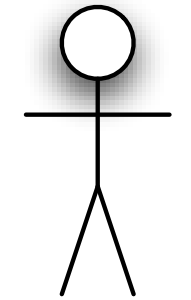


Alice

Producing Encrypted Ballot

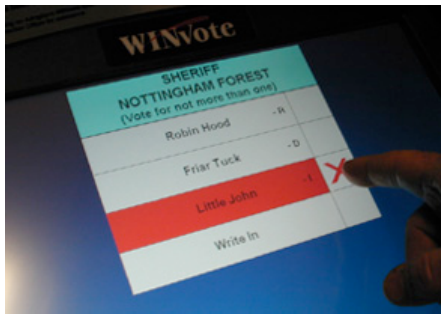


+

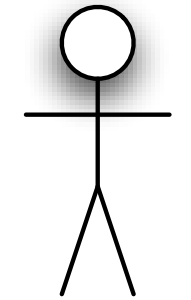


Alice

Producing Encrypted Ballot

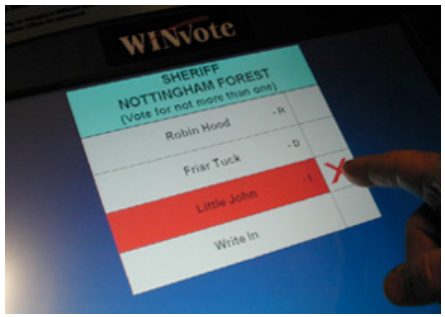


+

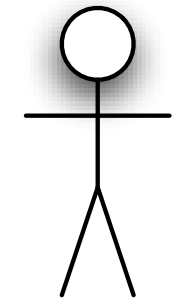


Alice

Producing Encrypted Ballot

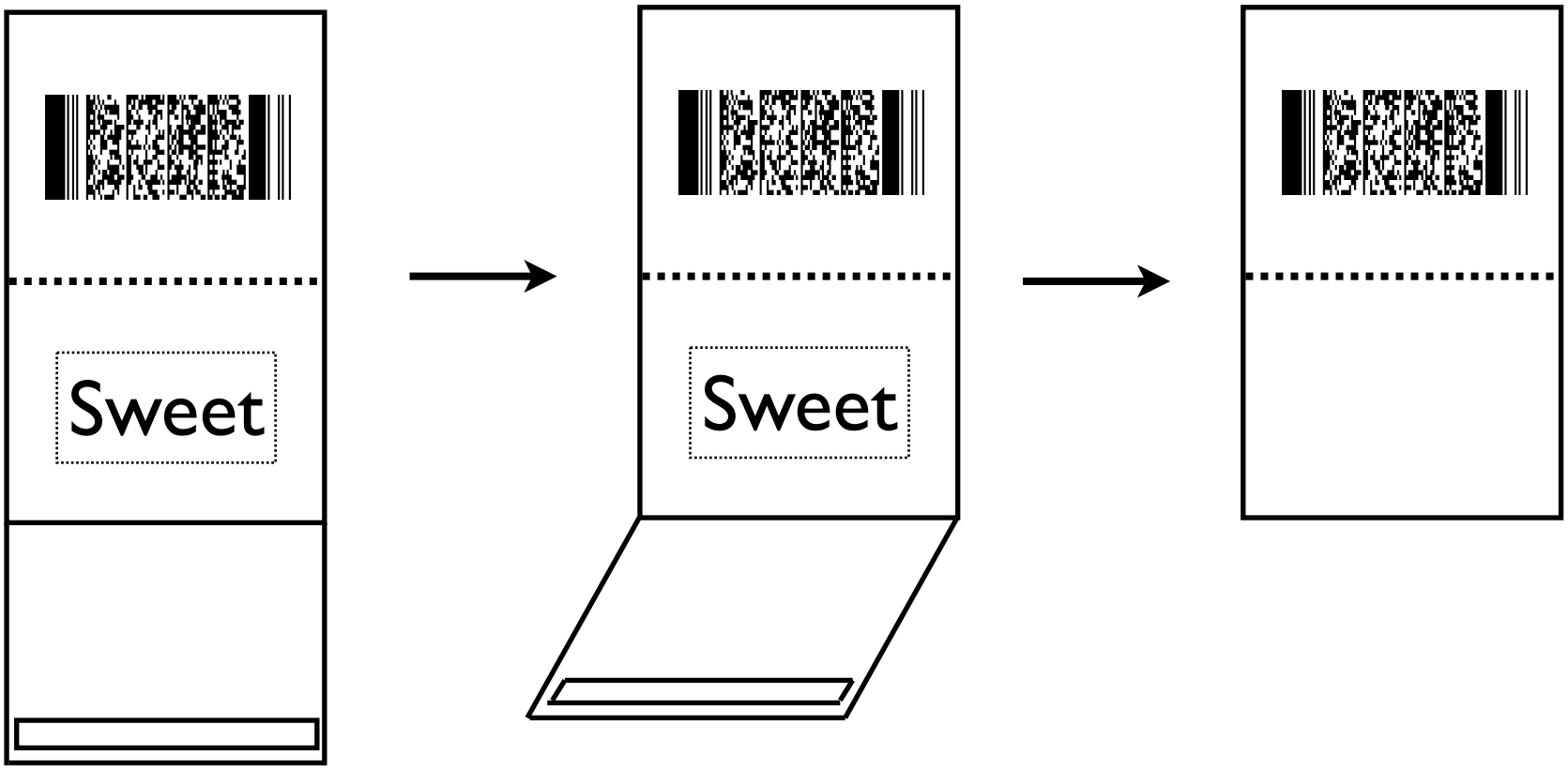


+

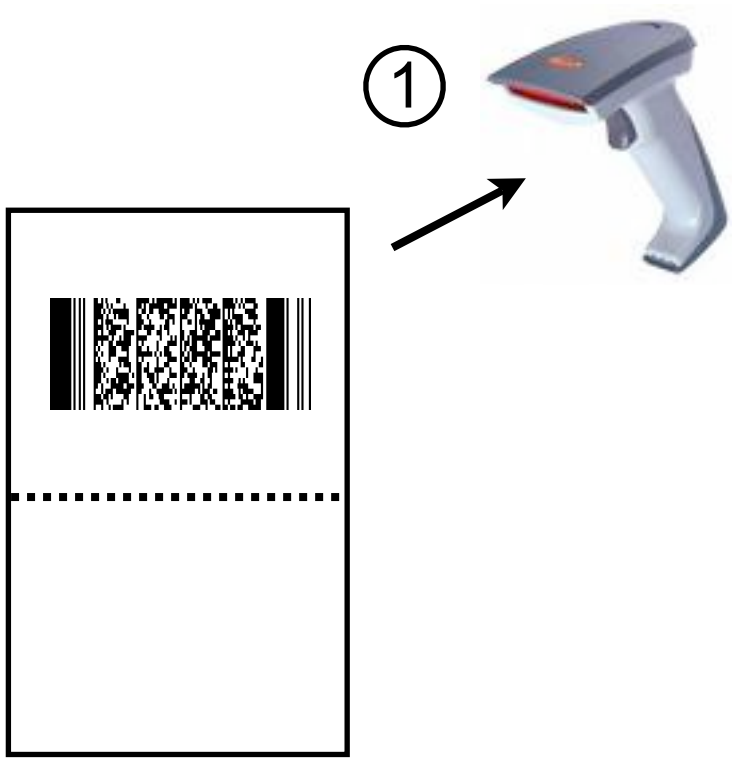


Alice

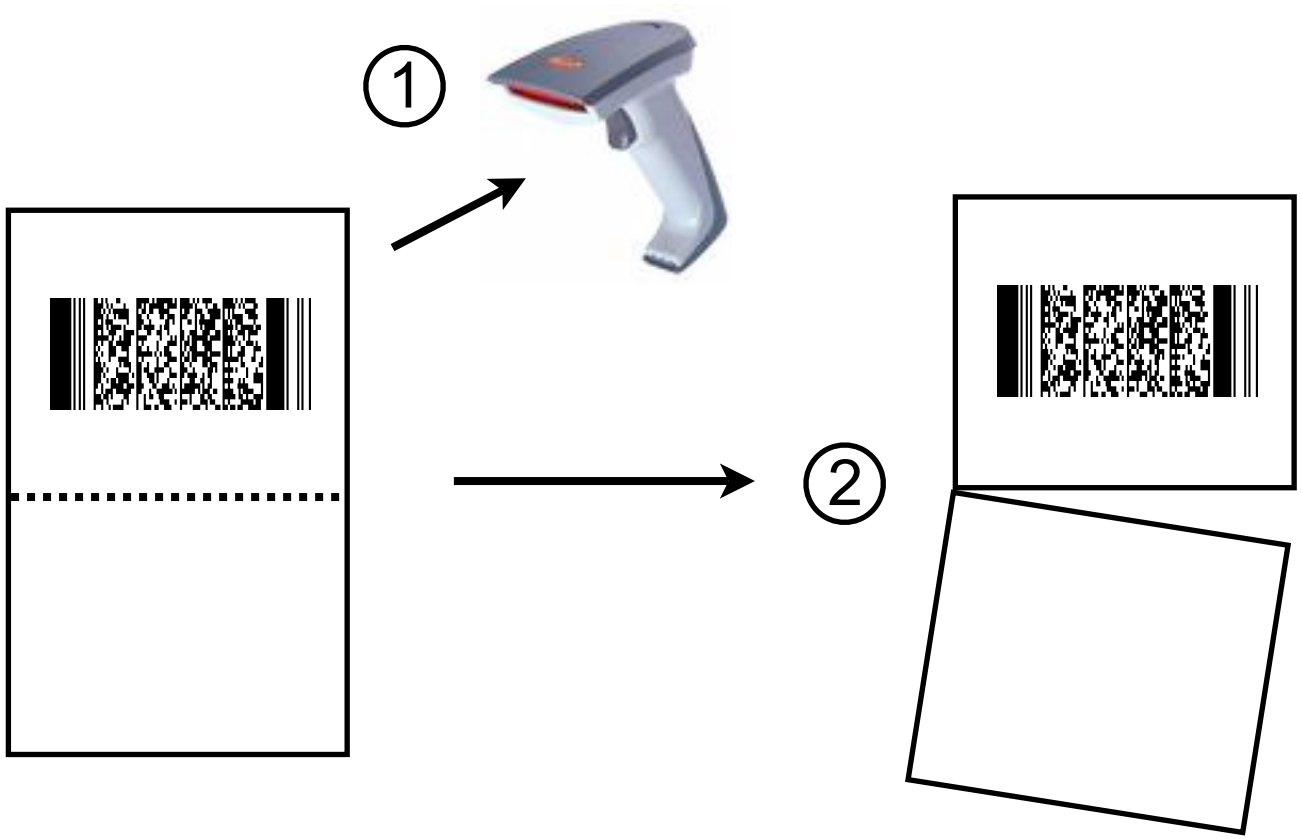
Encrypted Ballot



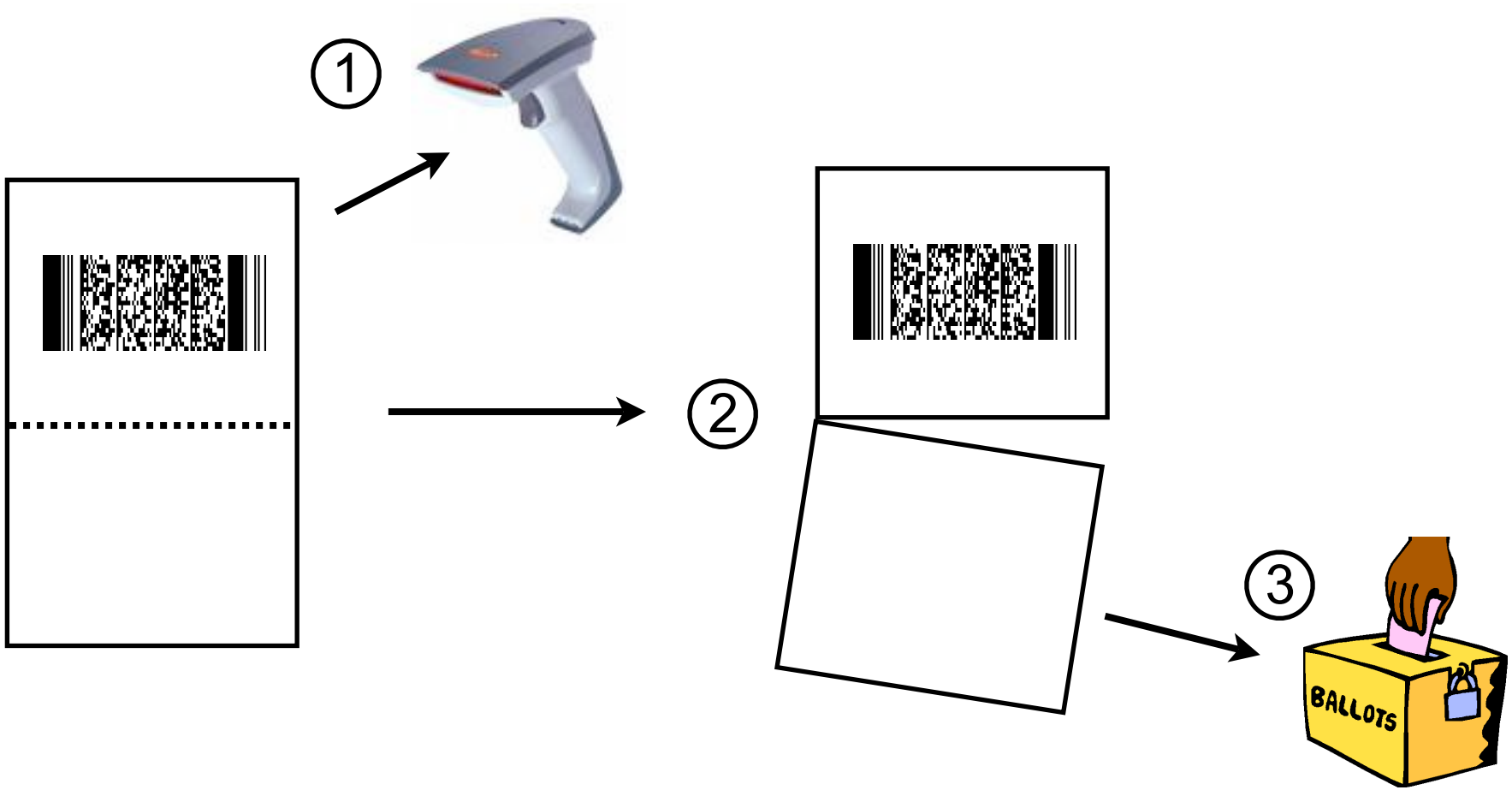
Ballot Casting



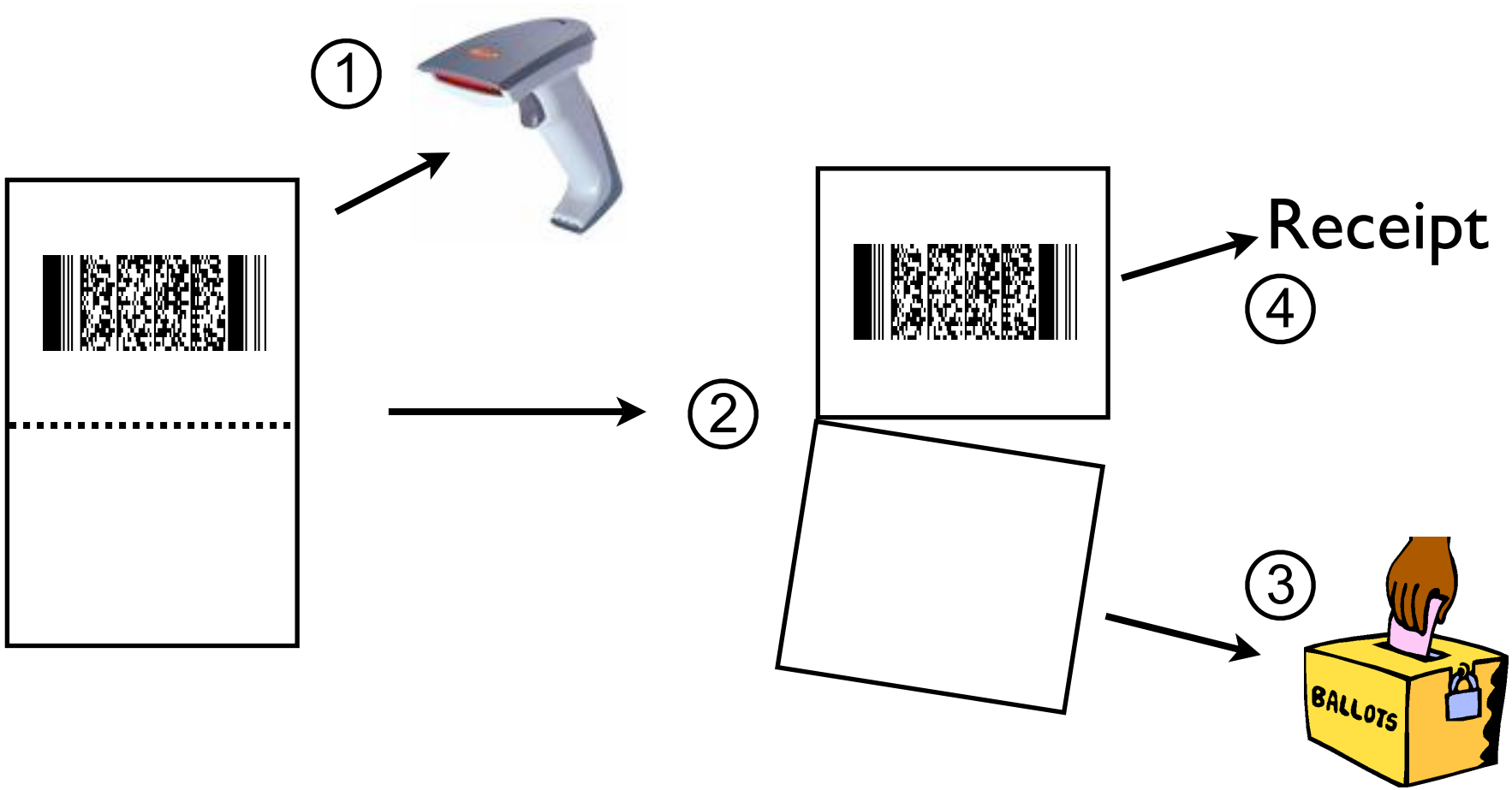
Ballot Casting



Ballot Casting



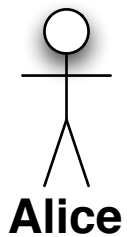
Ballot Casting



Verifying Consistency [Benaloh]

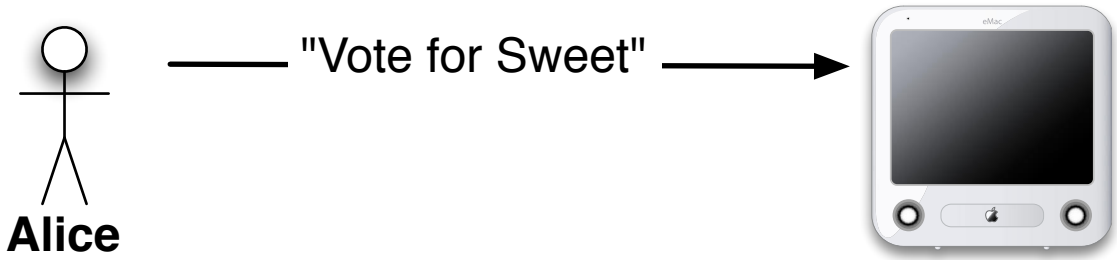
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



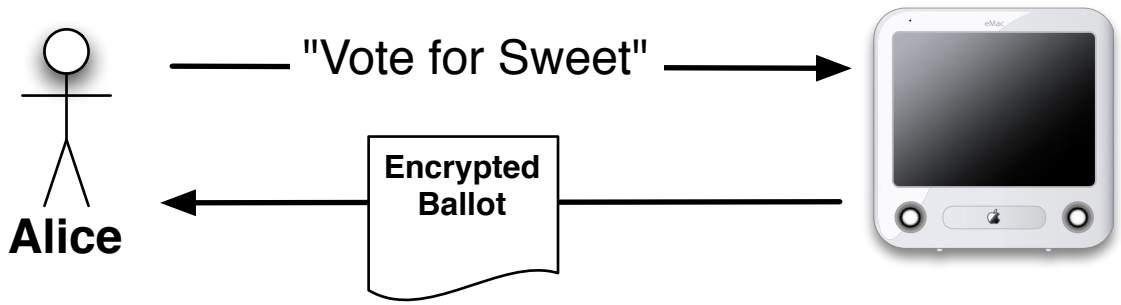
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



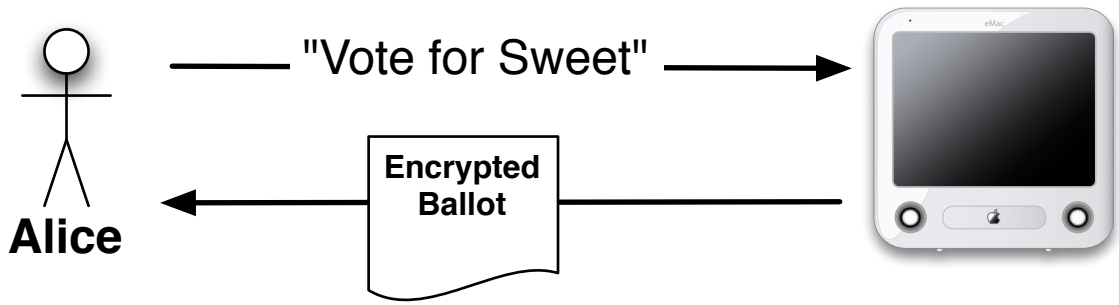
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



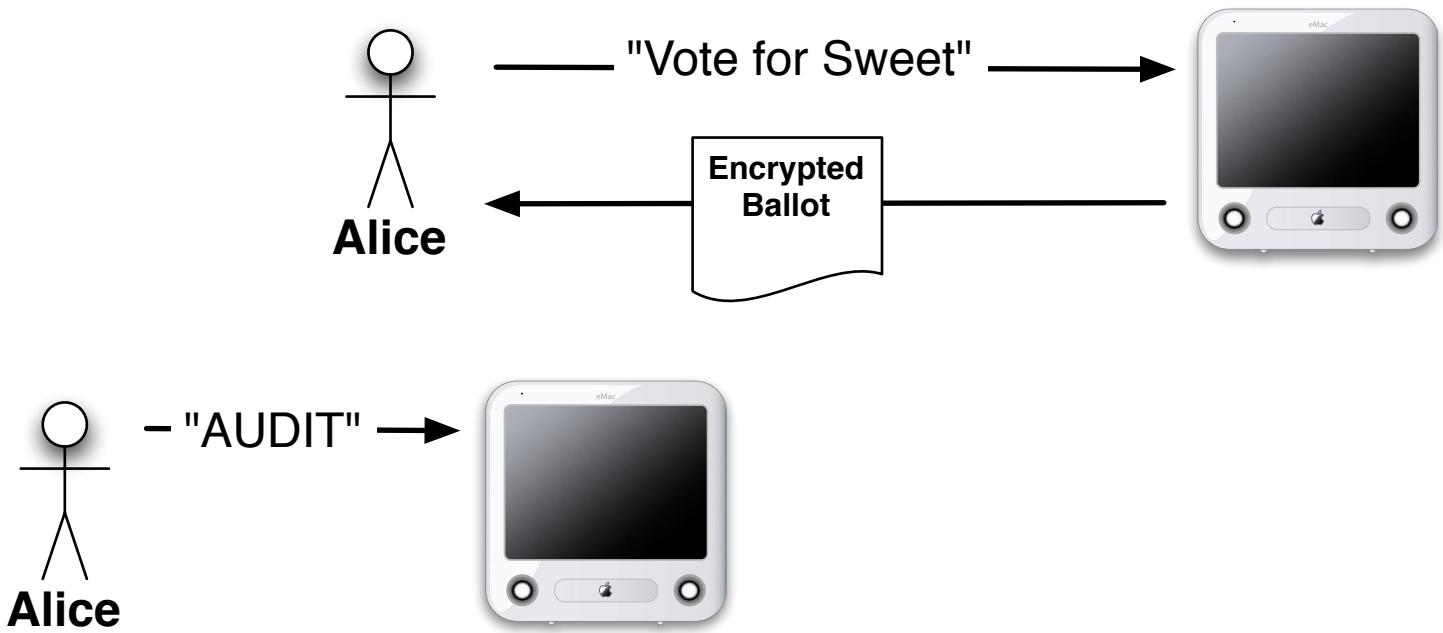
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



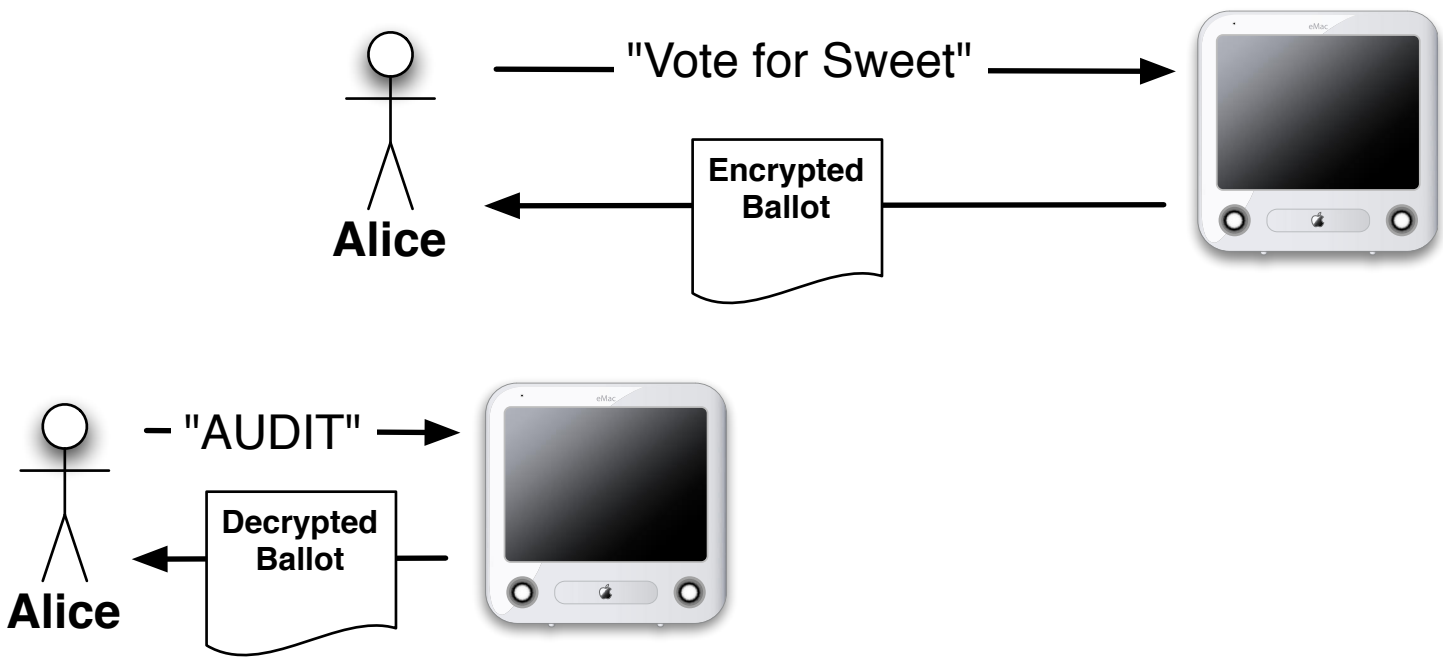
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



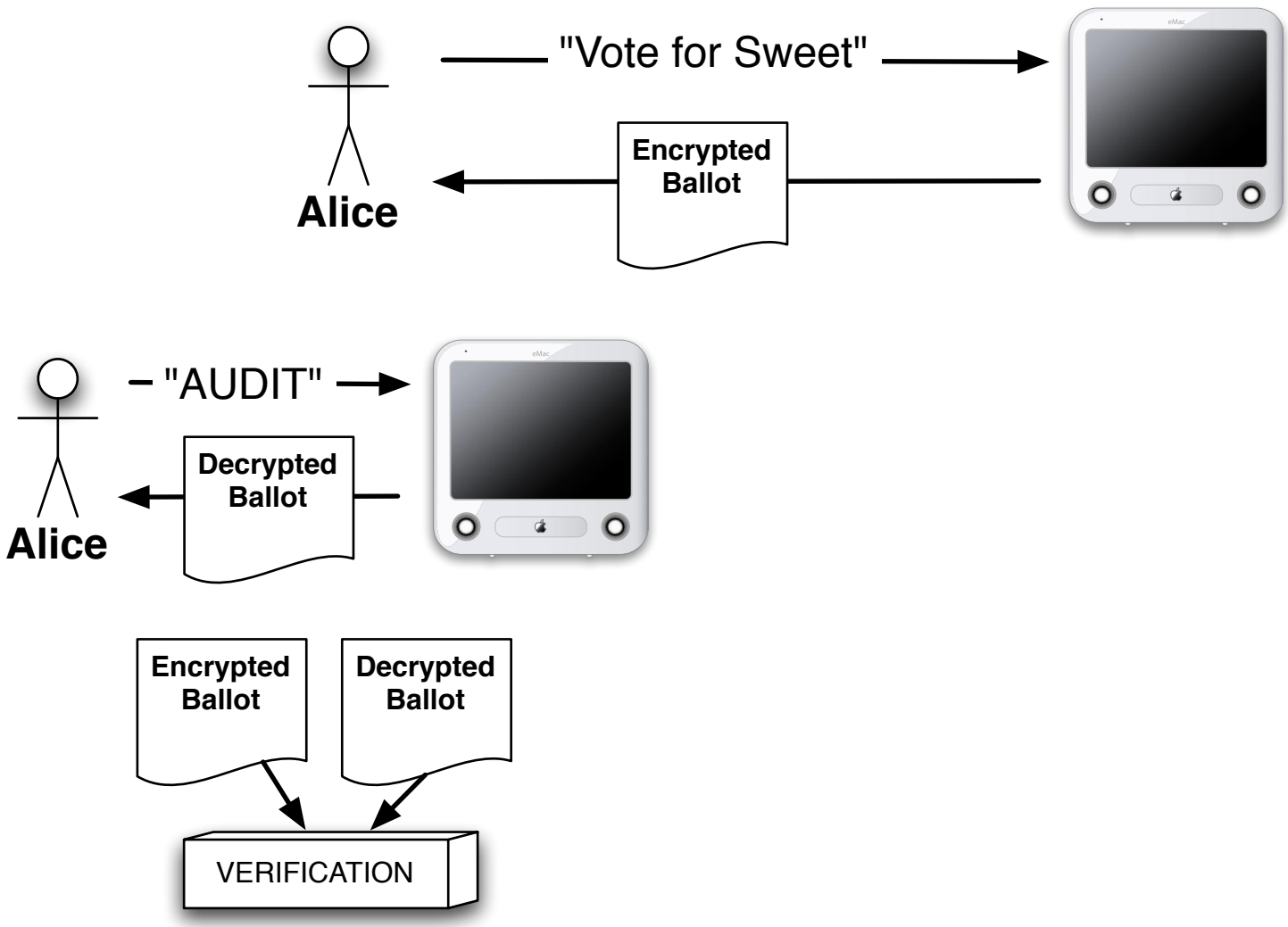
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



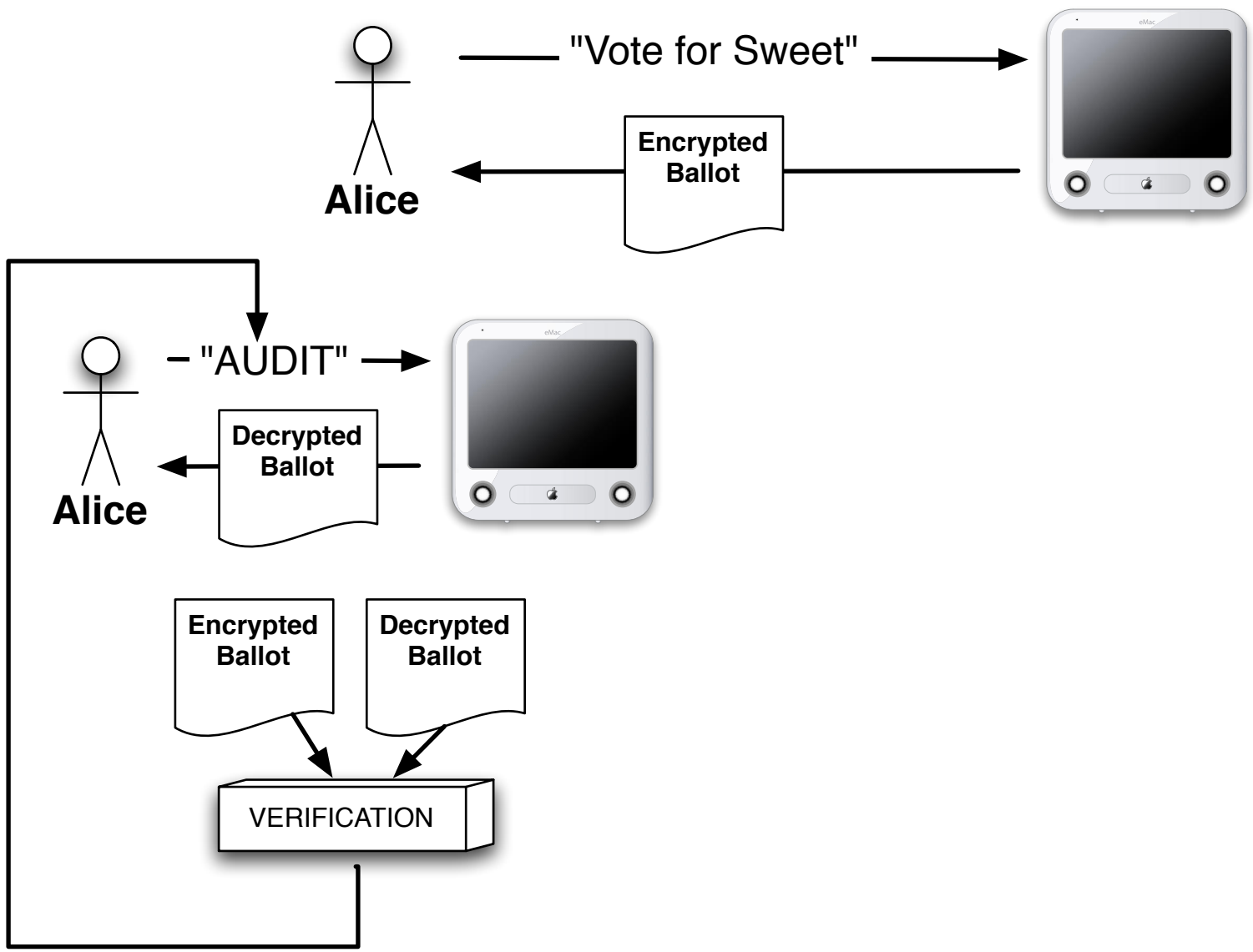
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



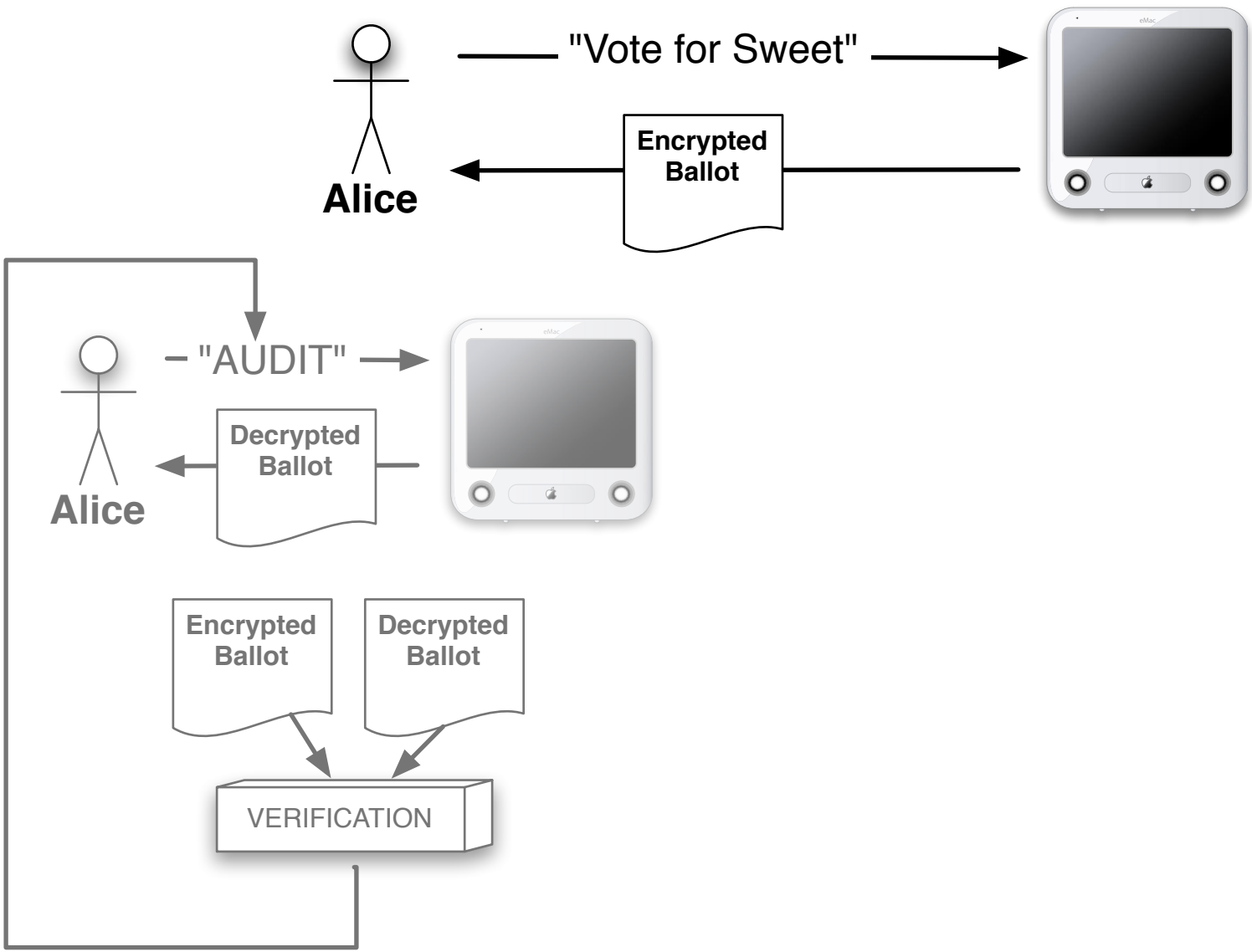
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



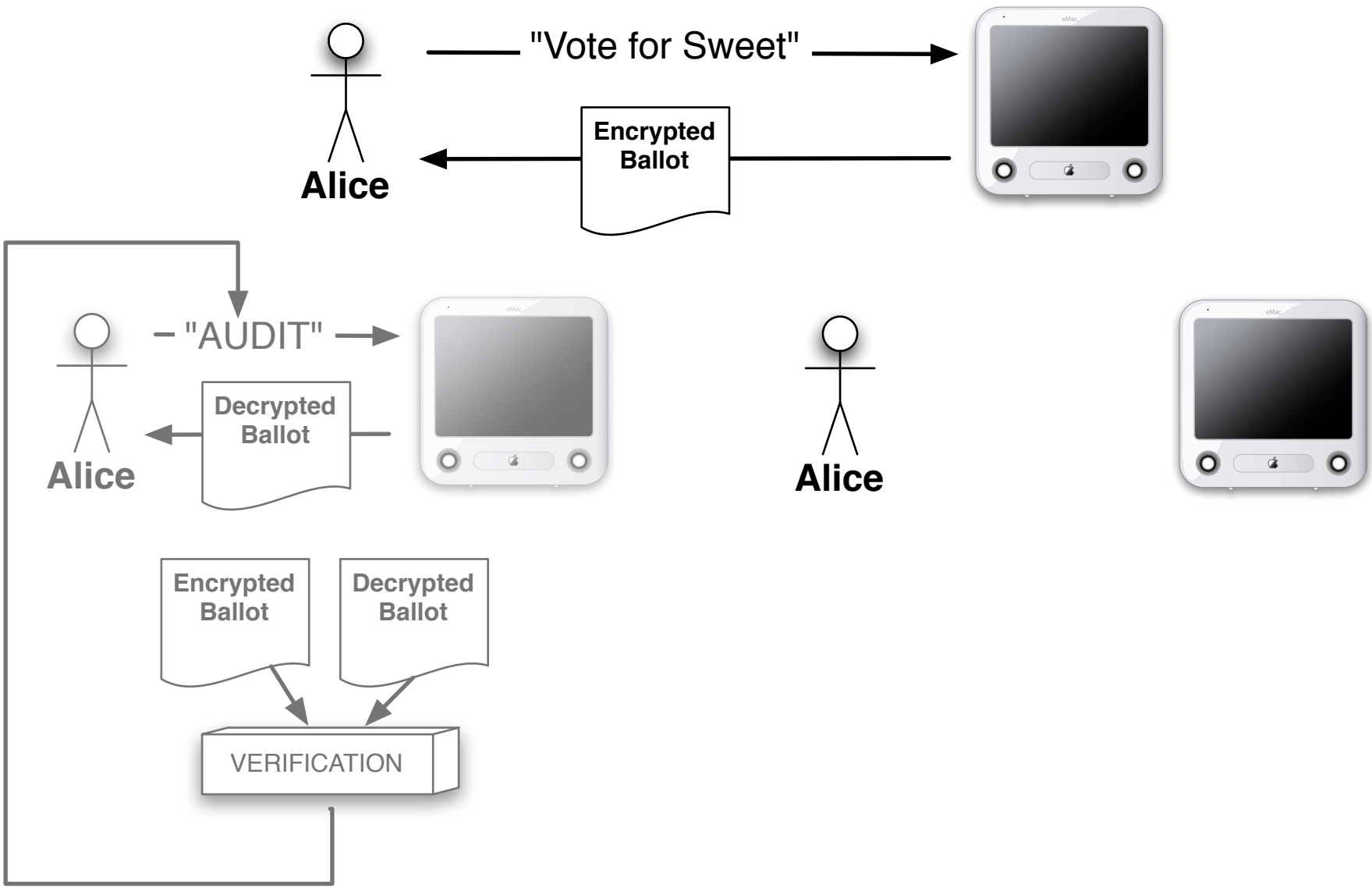
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



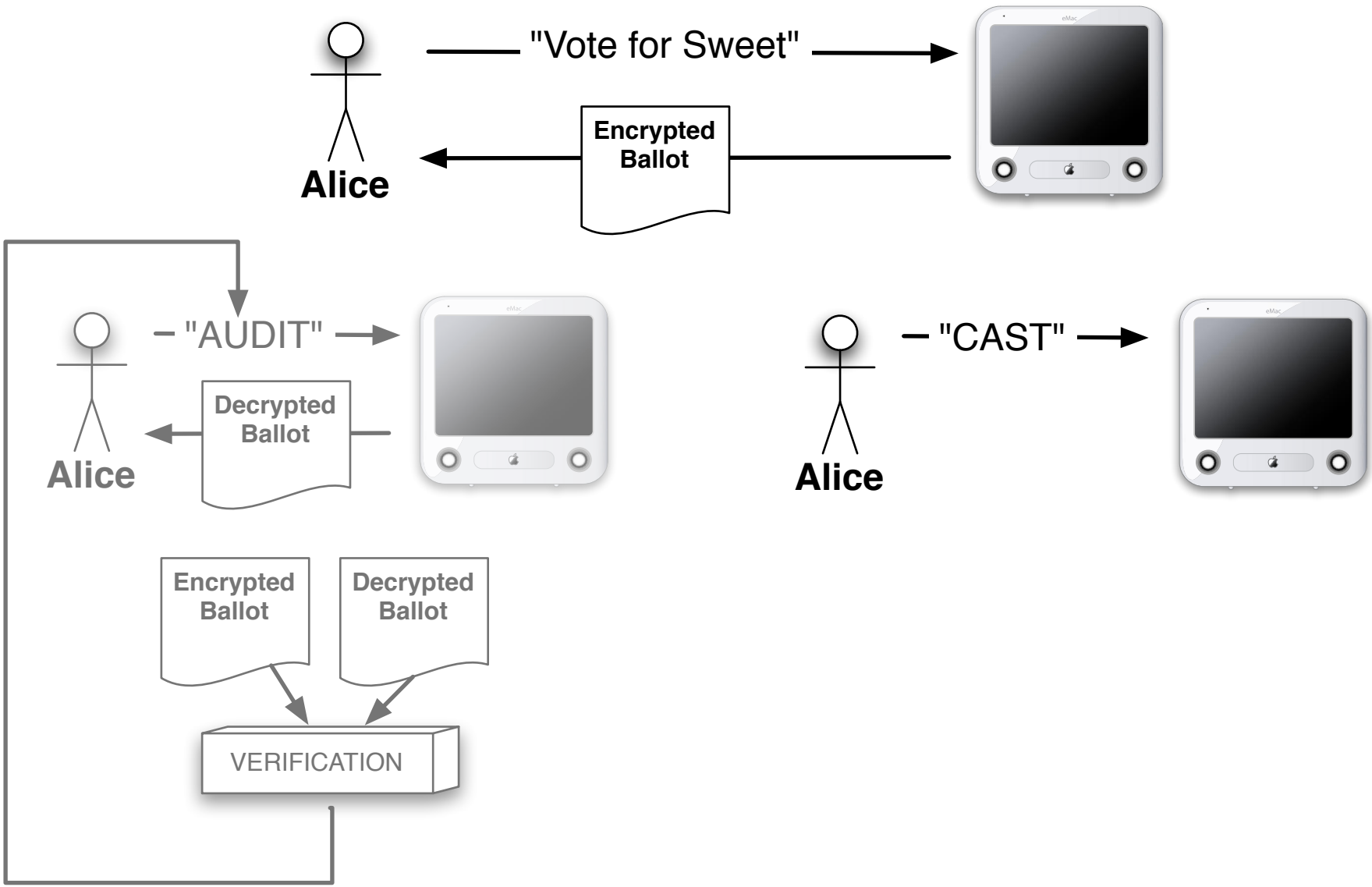
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



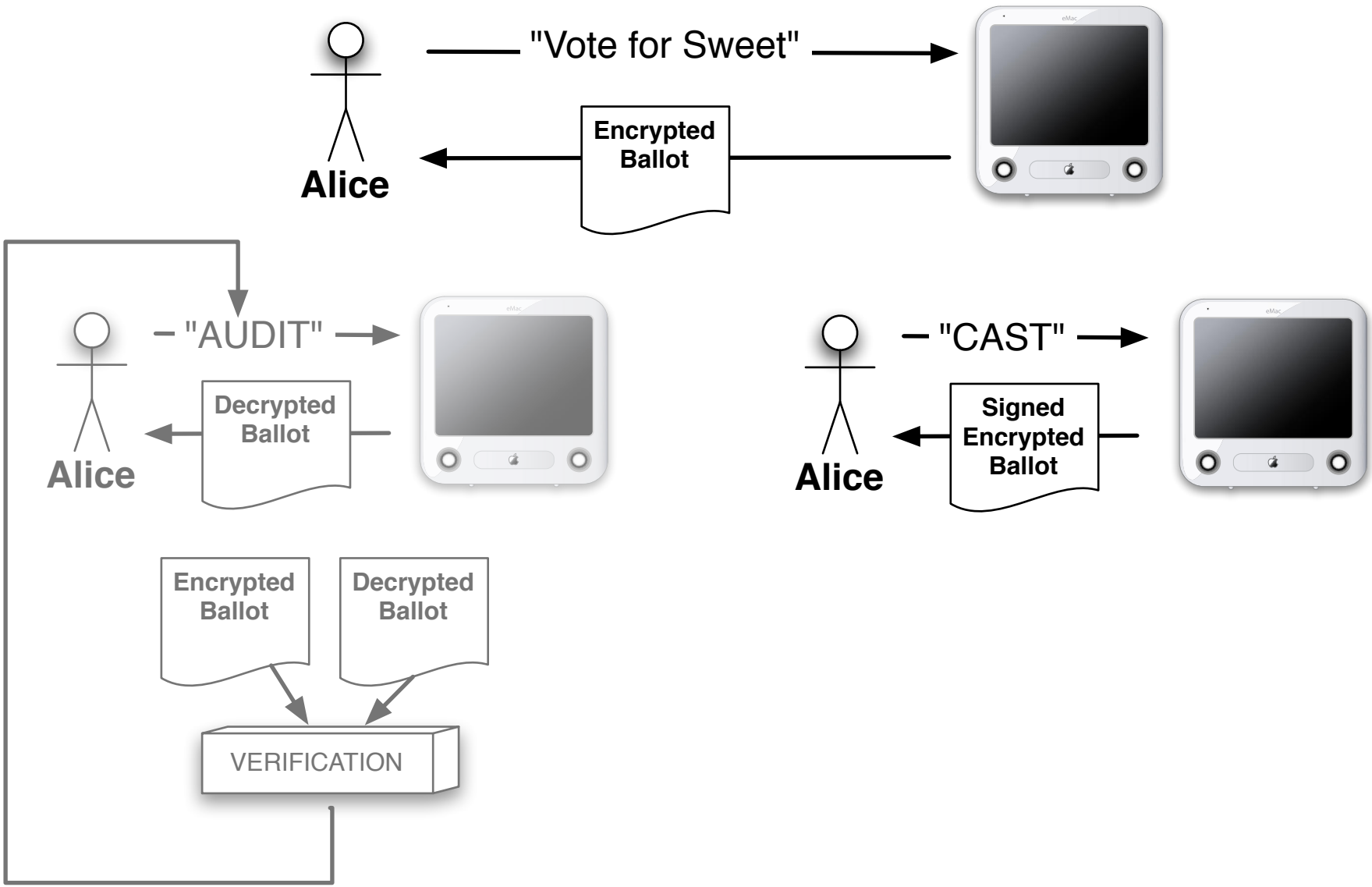
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



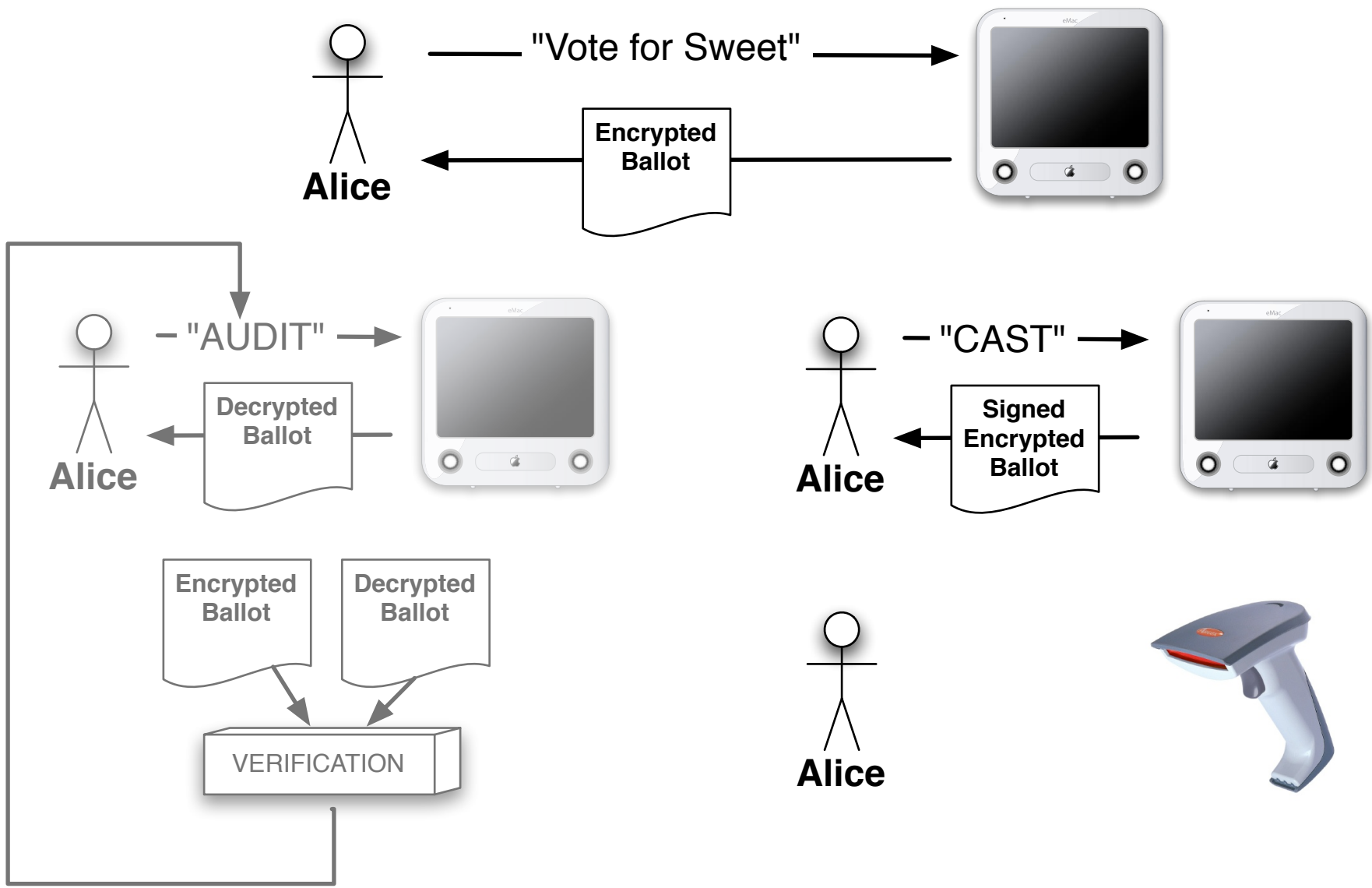
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



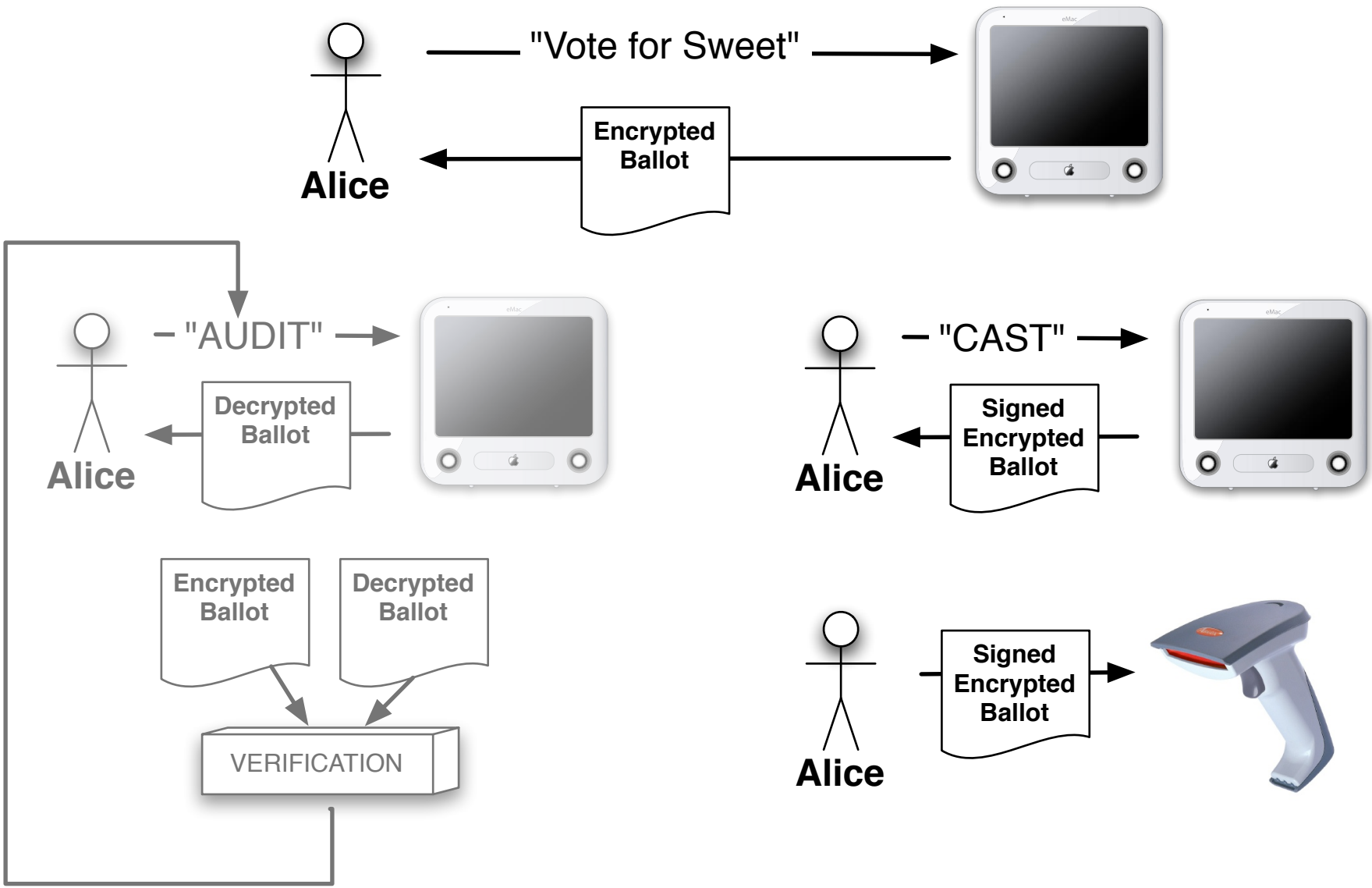
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]

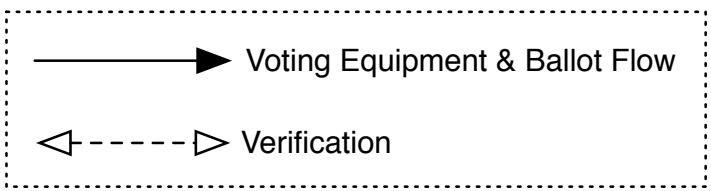


http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

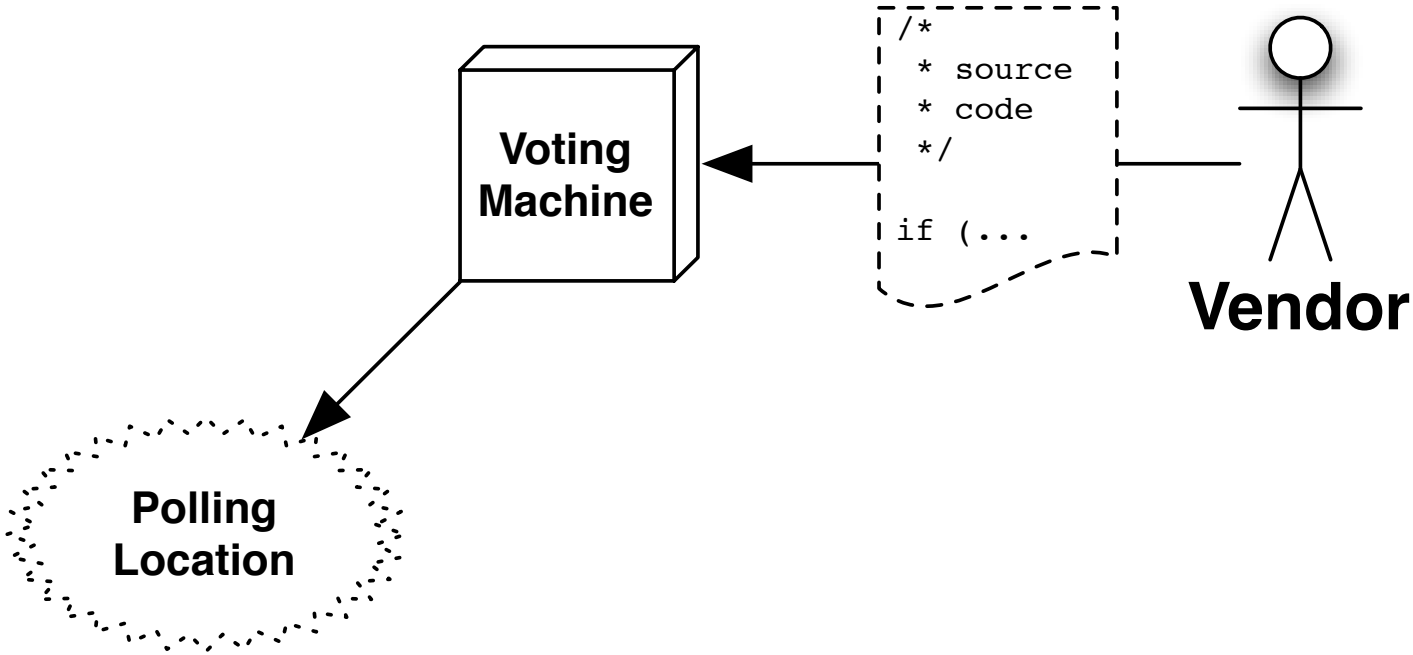
The Tallying Process

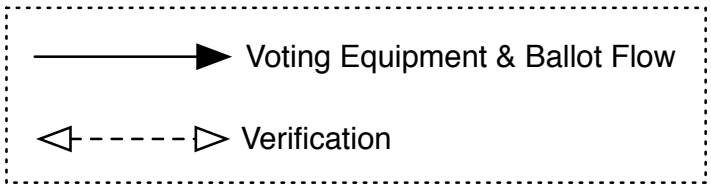
- **Paper tally**
- **Electronic tally**
  1. Homomorphic public-key encryption or mixnets
  2. Zero-knowledge proofs

Putting It Together

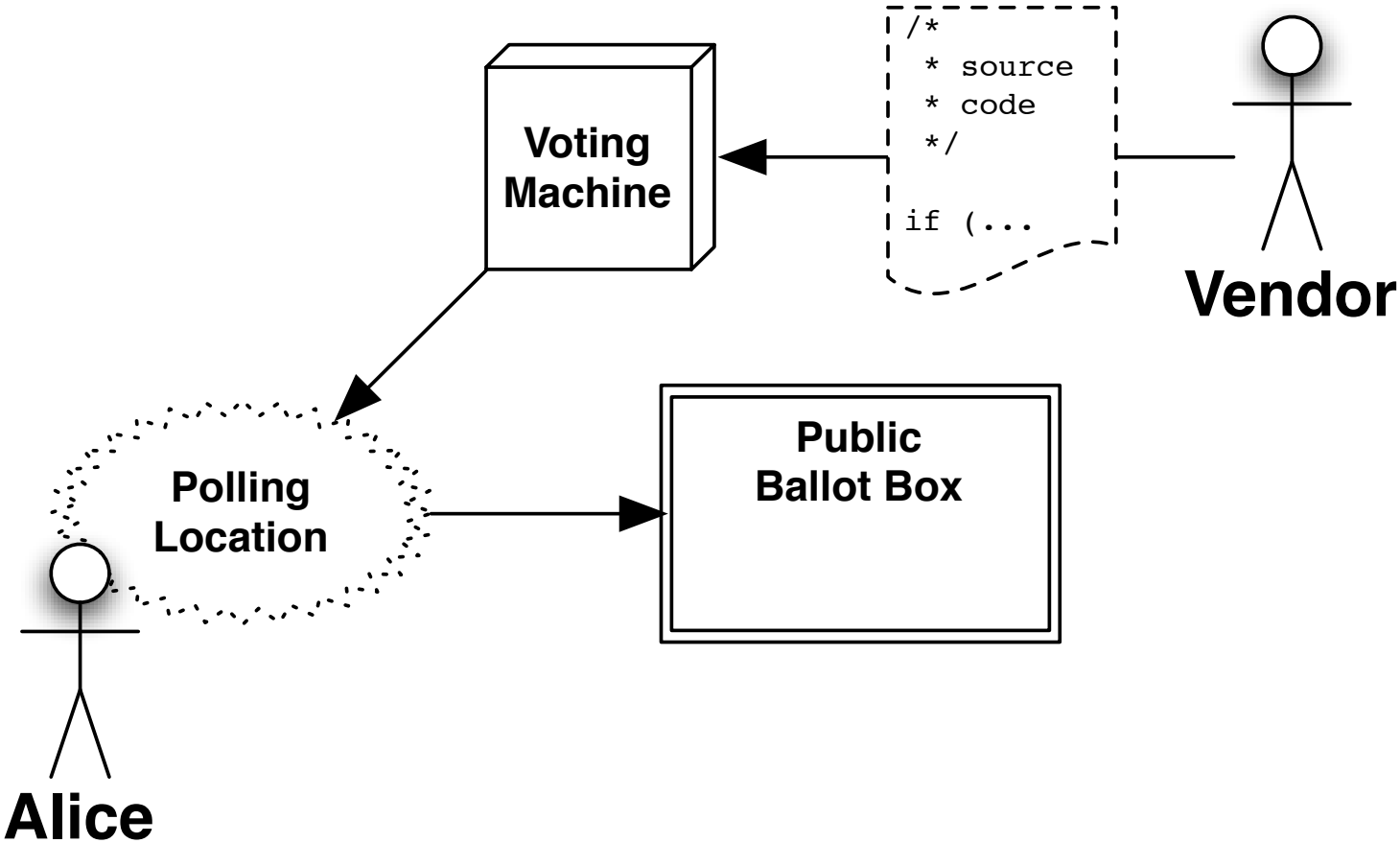


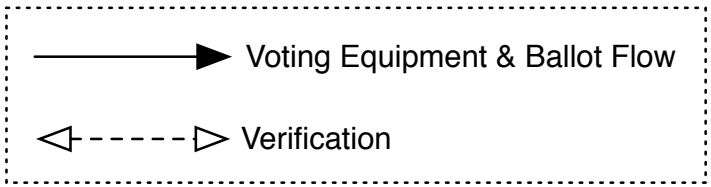
Putting It Together



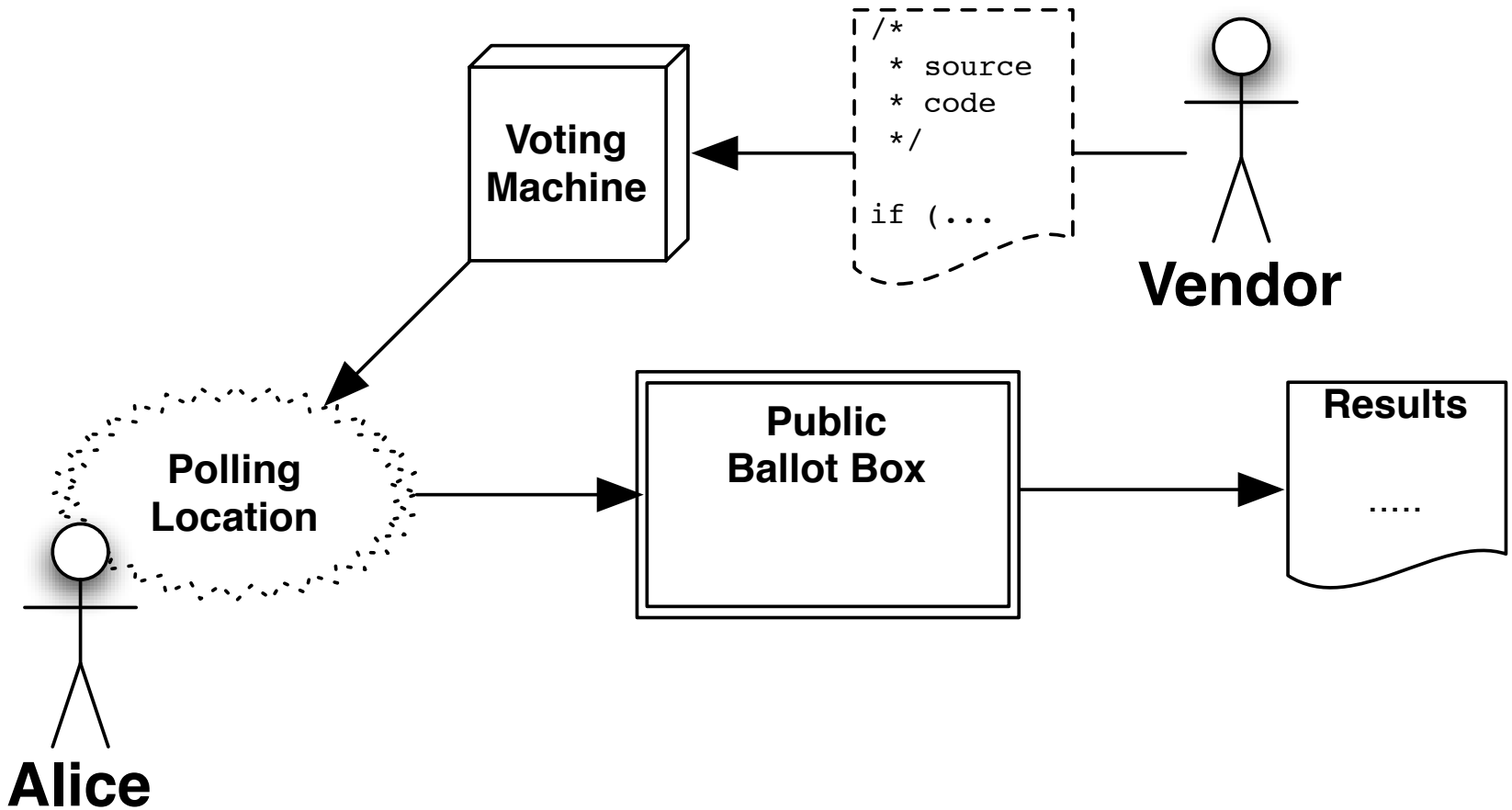


Putting It Together





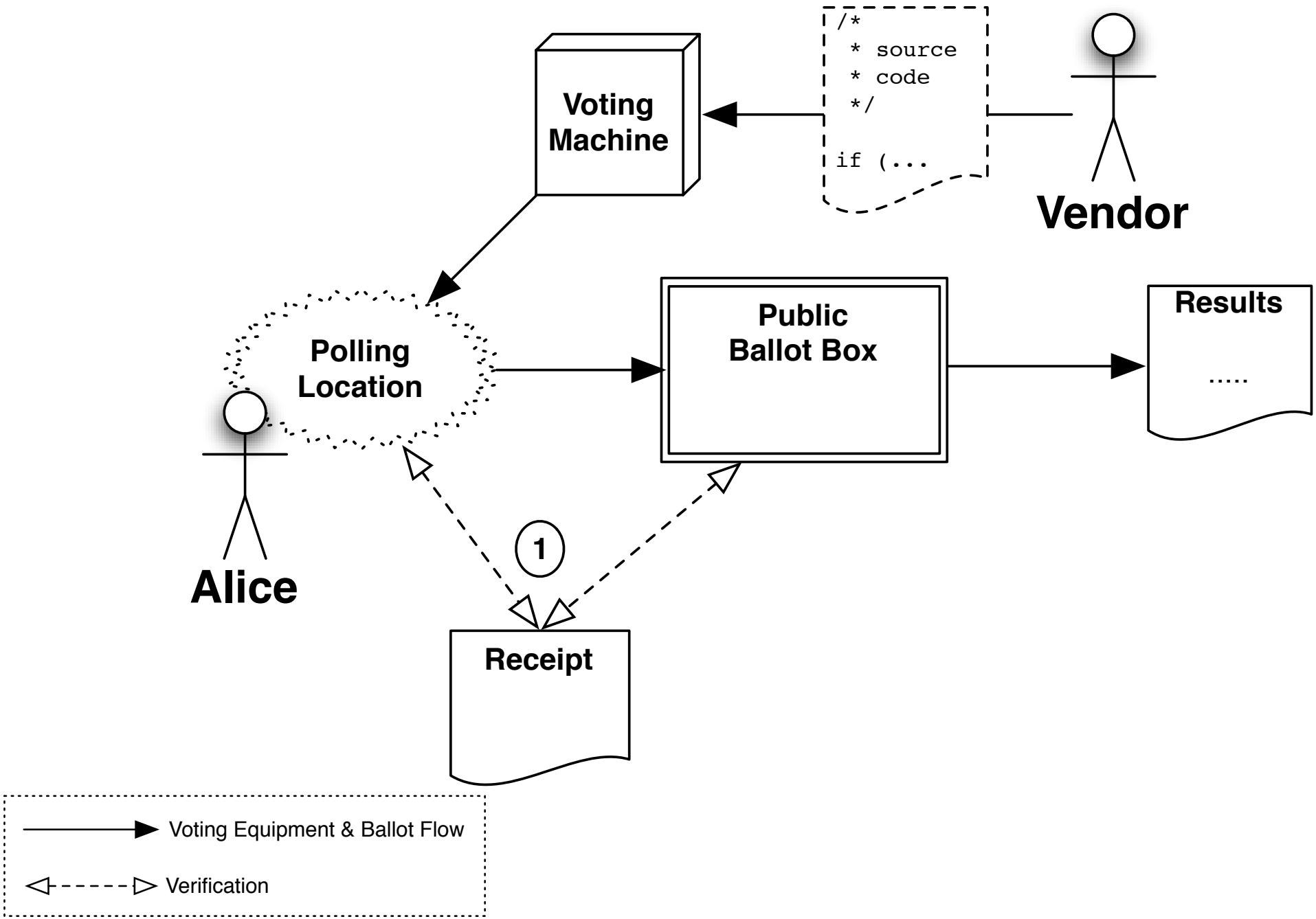
Putting It Together



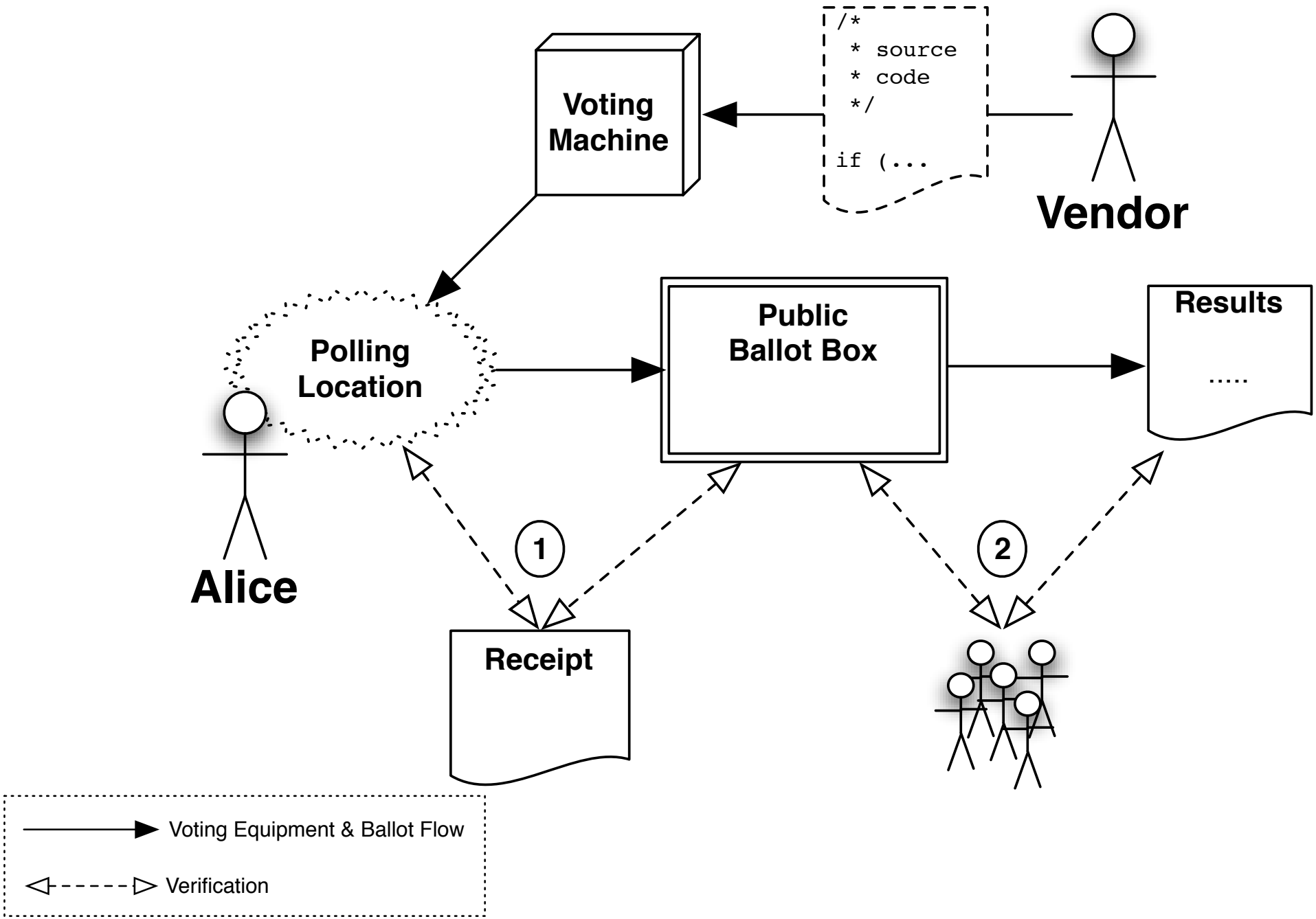
Voting Equipment & Ballot Flow

Verification

Putting It Together



Putting It Together



Open-Audit Elections

- **Alice** verifies **her vote**.
- **Everyone** verifies **the tally**.
- **Incoercibility** is enforced.

Open-Audit Elections

- **Alice** verifies **her vote**.
- **Everyone** verifies **the tally**.
- **Incoercibility** is enforced.

Anyone can Audit.

Open Audit Voting: Helios (Ben Adida, 2009)

Helios Voting Booth

Princeton Fall 2009 Test Election

Election Fingerprint:
qnc0eX00k7snXPBTjX9k258J981AY163KP2m8Nyj3+o

Election to evaluate Helios for Princeton Student Elections

(1) Select	(2) Encrypt	(3) Submit

Question #1 of 3

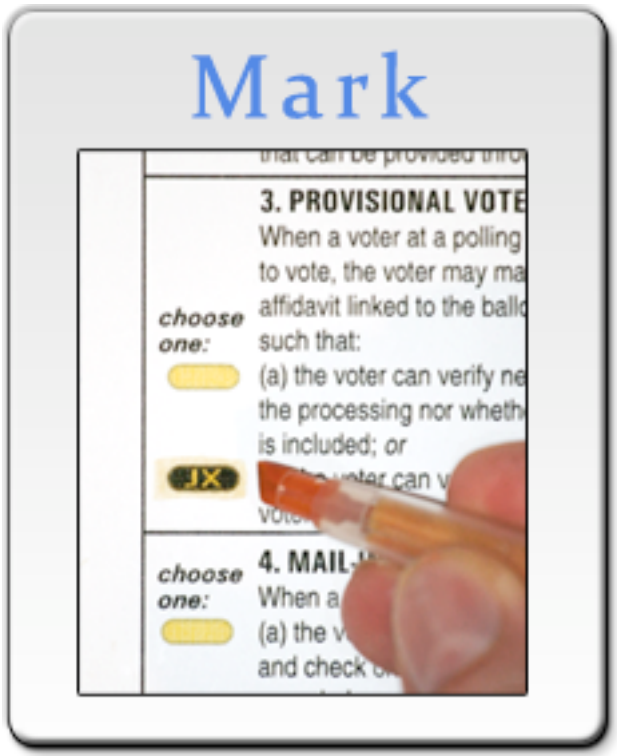
Who should be the Class of 2013 President?

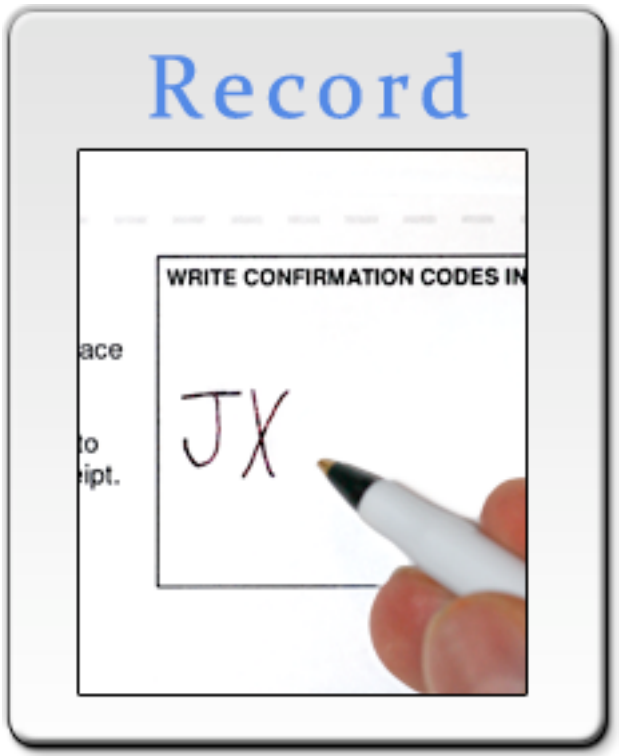
(select up to 1 answer)

- ☐ Miss Piggy
- ☐ Jerry Seinfeld
- ☐ Bugs Bunny
- ☐ Chuck Norris

Next

Open Audit Voting: Scantegrity II (Chaum et al., 2009)





Questions?