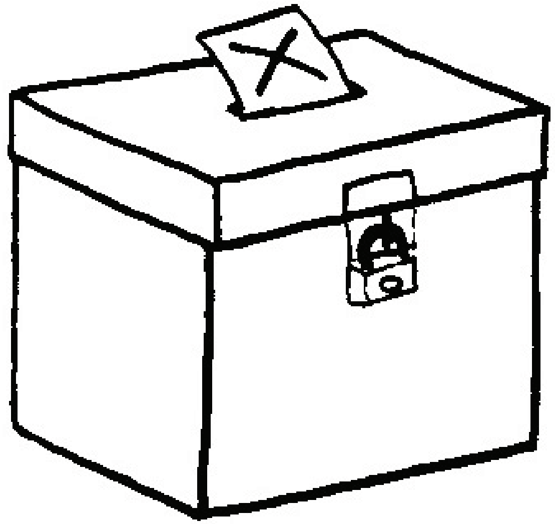


Cryptographic elections

Alon Rosen
IDC Herzliya

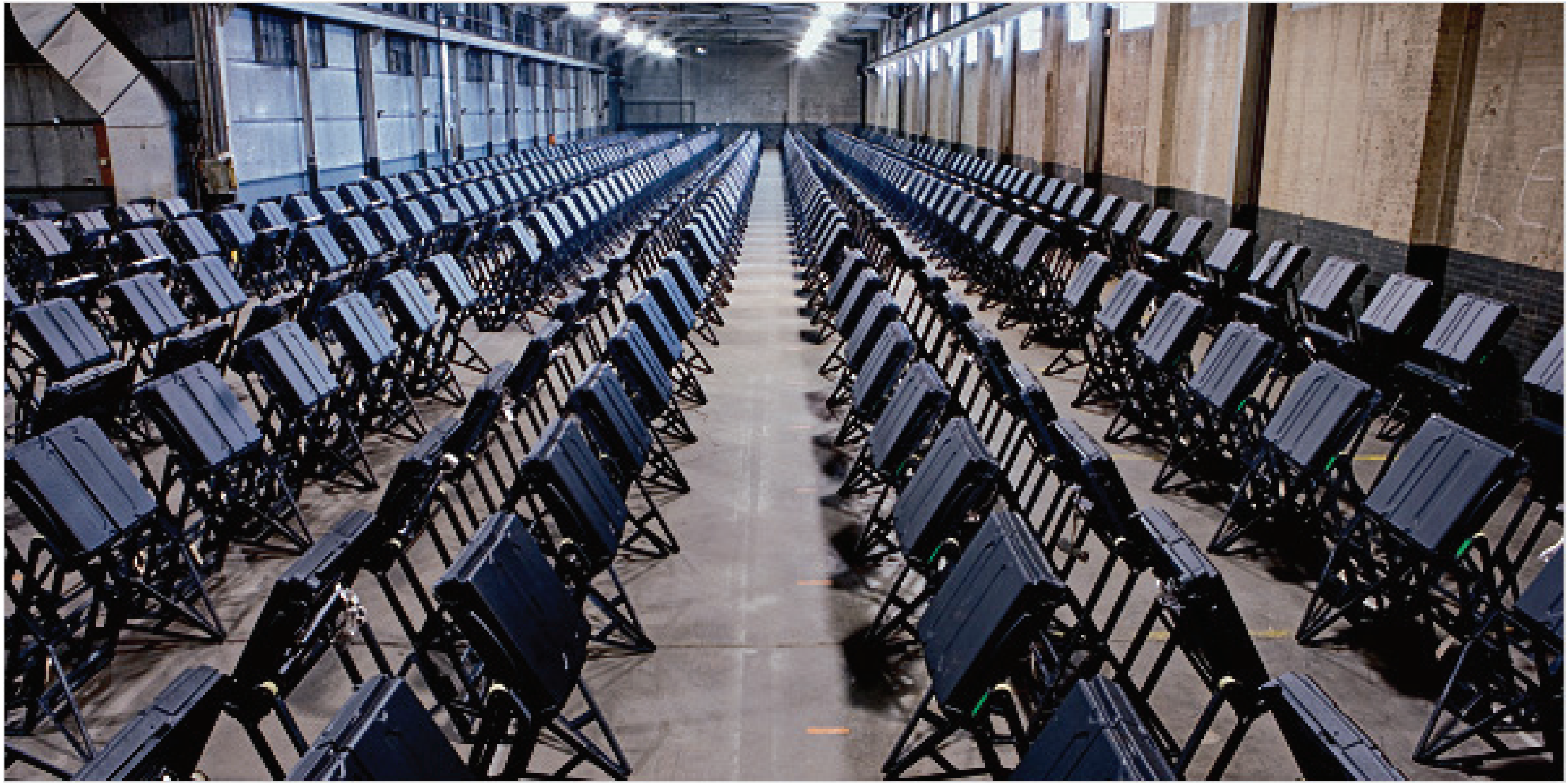
September 14th, 2008

Thanks

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

This Talk

- Current voting technology has serious flaws.
- Voting is hard.
- Commonly proposed solutions fall short.
- Cryptographic voting has the potential to revolutionize how we audit elections.

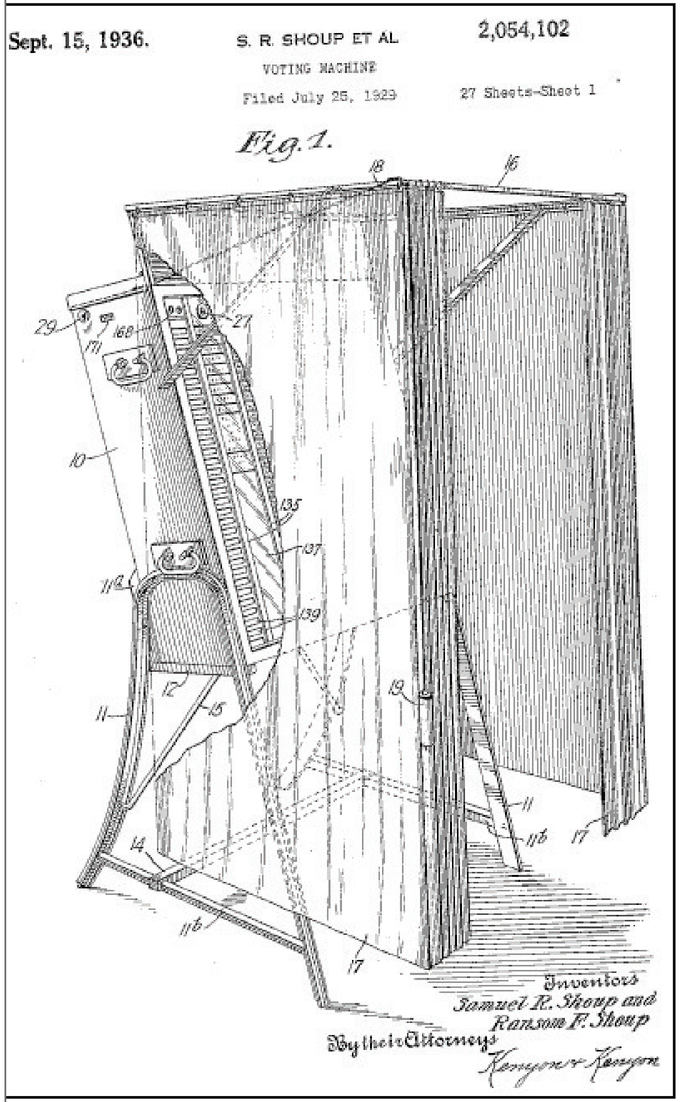


http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html

Voting in the US

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

Voting in the US



Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102

VOTING MACHINE

Filed July 25, 1929 27 Sheets-Sheet 1

Fig. 1.

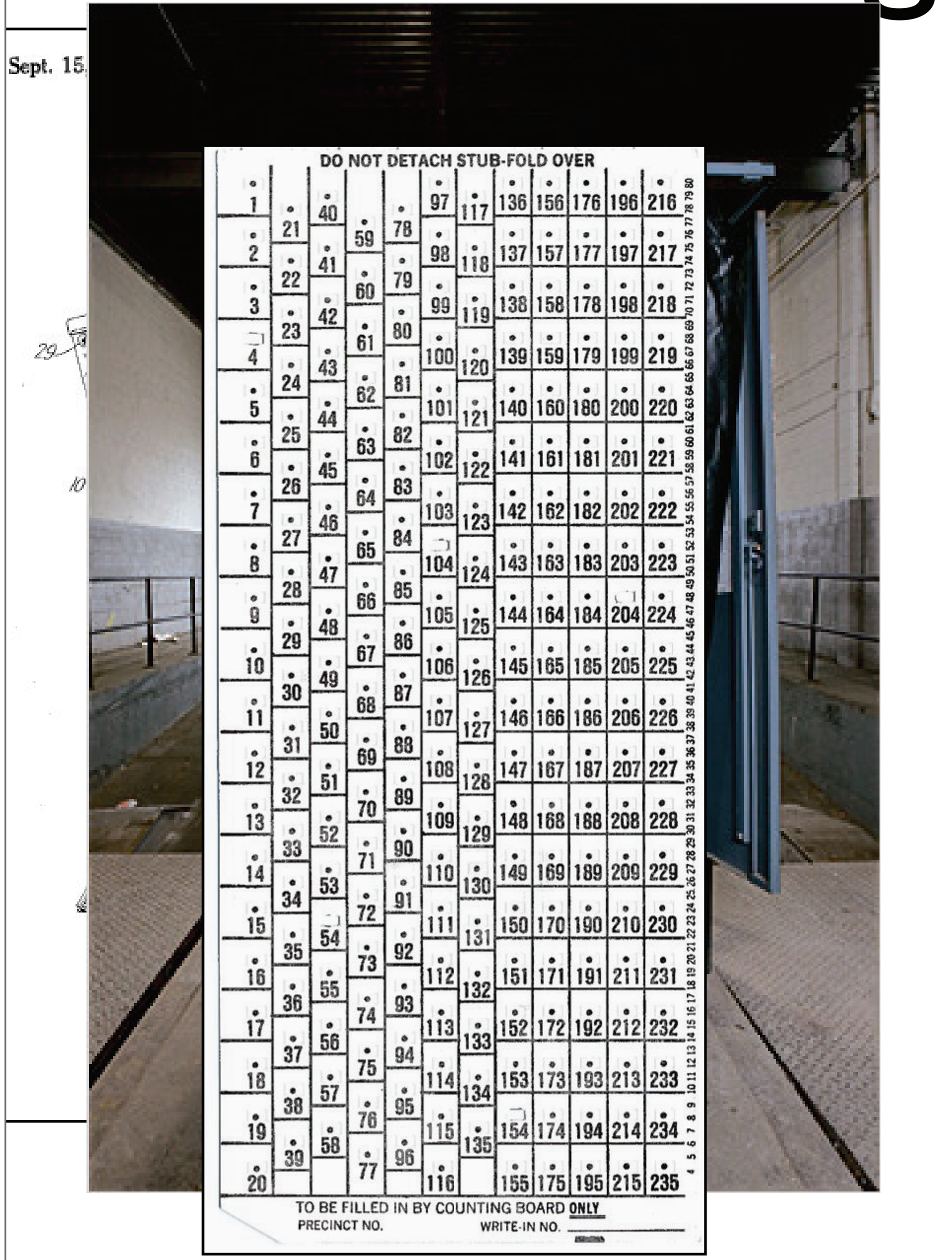
Inventors
Samuel R. Shoup and
Ransom F. Shoup
By their Attorneys
Kenyon & Kenyon

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

Voting in the US

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

Voting in the US



DO NOT DETACH STUB-FOLD OVER

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39

40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58

59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77

78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96

97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116

117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135

136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155

156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175

176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195

196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215

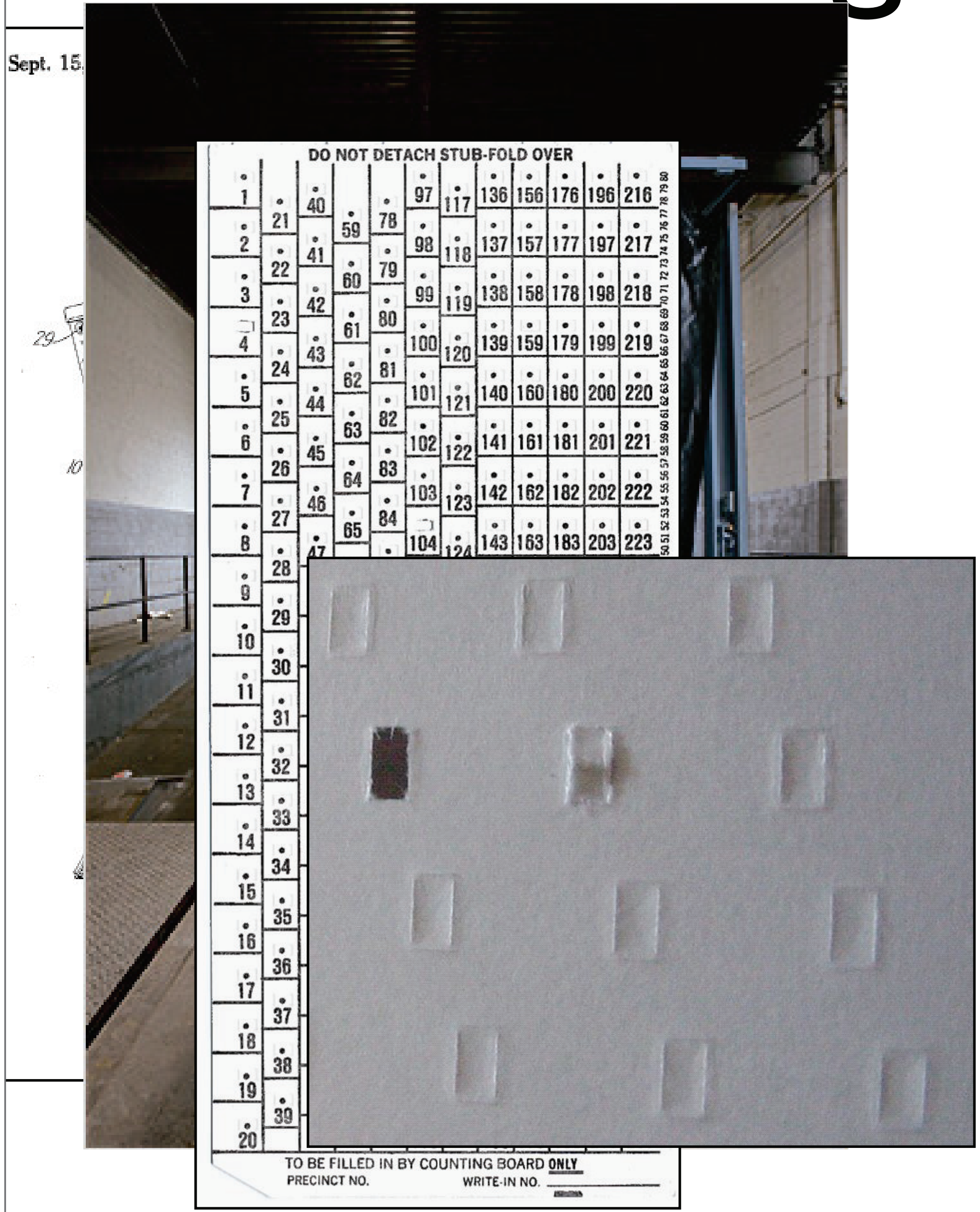
216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235

TO BE FILLED IN BY COUNTING BOARD ONLY

PRECINCT NO. WRITE-IN NO.

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

Voting in the US



Sept. 15,

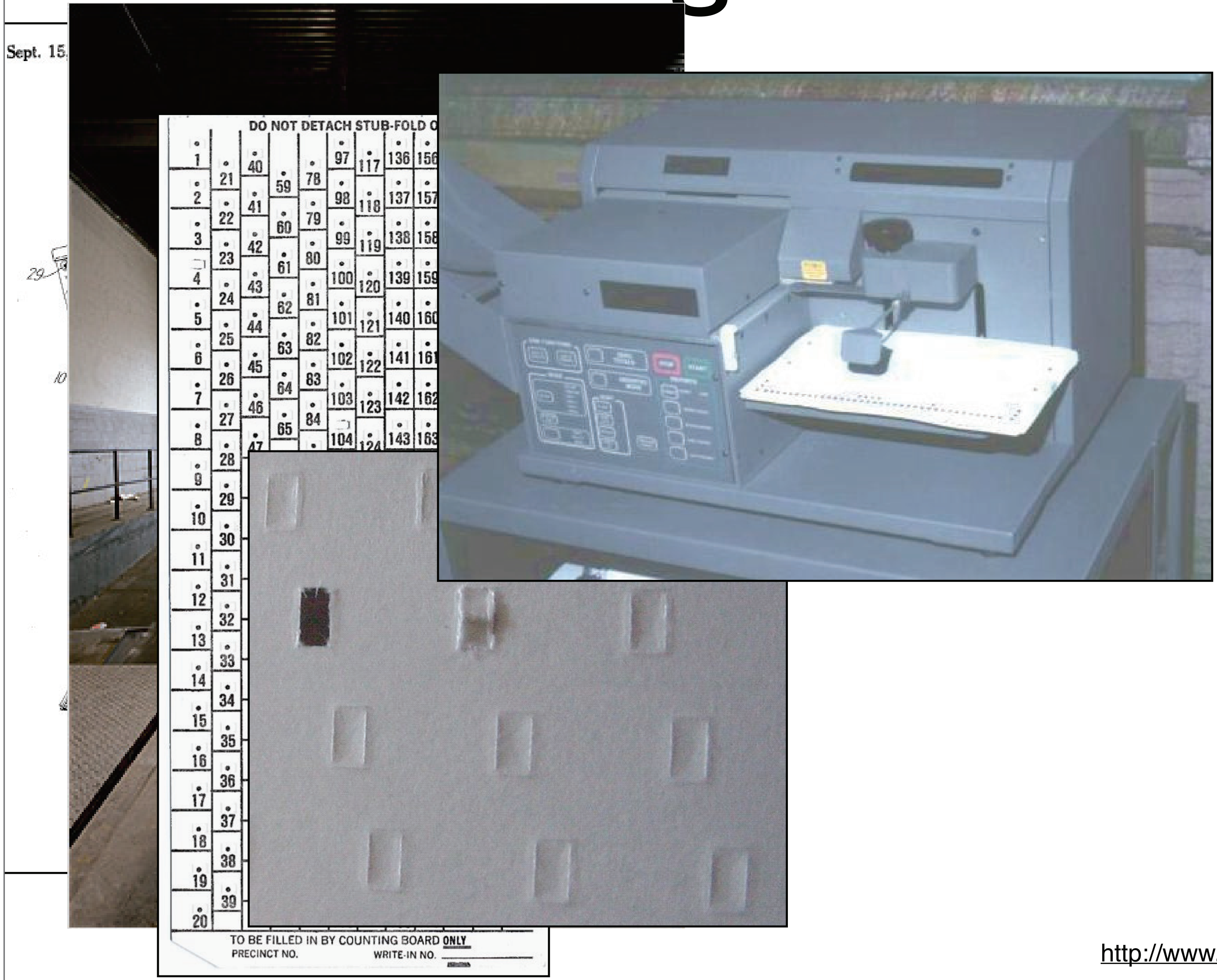
DO NOT DETACH STUB-FOLD OVER

TO BE FILLED IN BY COUNTING BOARD ONLY

PRECINCT NO. WRITE-IN NO.

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

Voting in the US


Sept. 15,
DO NOT DETACH STUB-FOLD O
TO BE FILLED IN BY COUNTING BOARD ONLY
PRECINCT NO.
WRITE-IN NO.

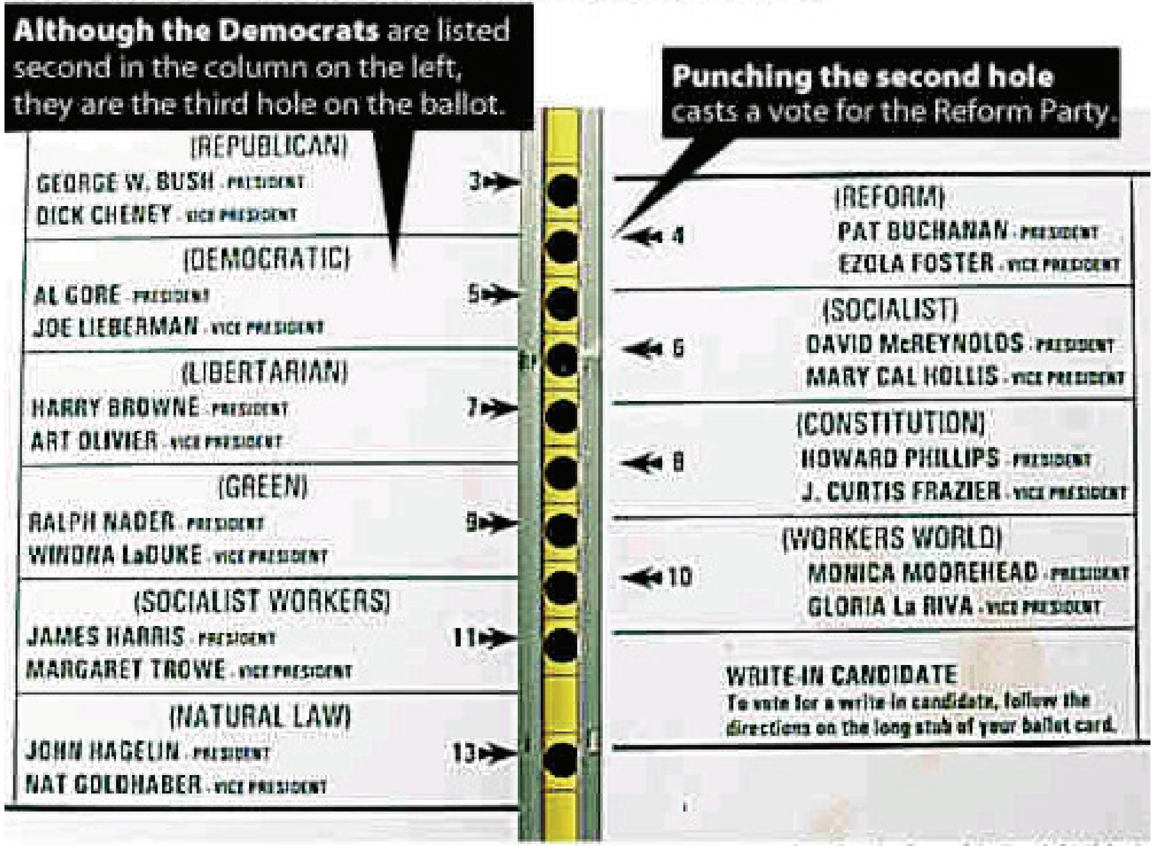
http://www.cs.uiowa.edu/~jones/voting/pictures/

Voting in the US

Sept. 15
DO NOT DETACH STUB-FOLD O
TO BE FILLED IN BY COUNTING BOARD ONLY
PRECINCT NO.
WRITE-IN NO.
DIEBOLD
INSERT BALLOT HERE

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

Confusion over Palm Beach County ballot

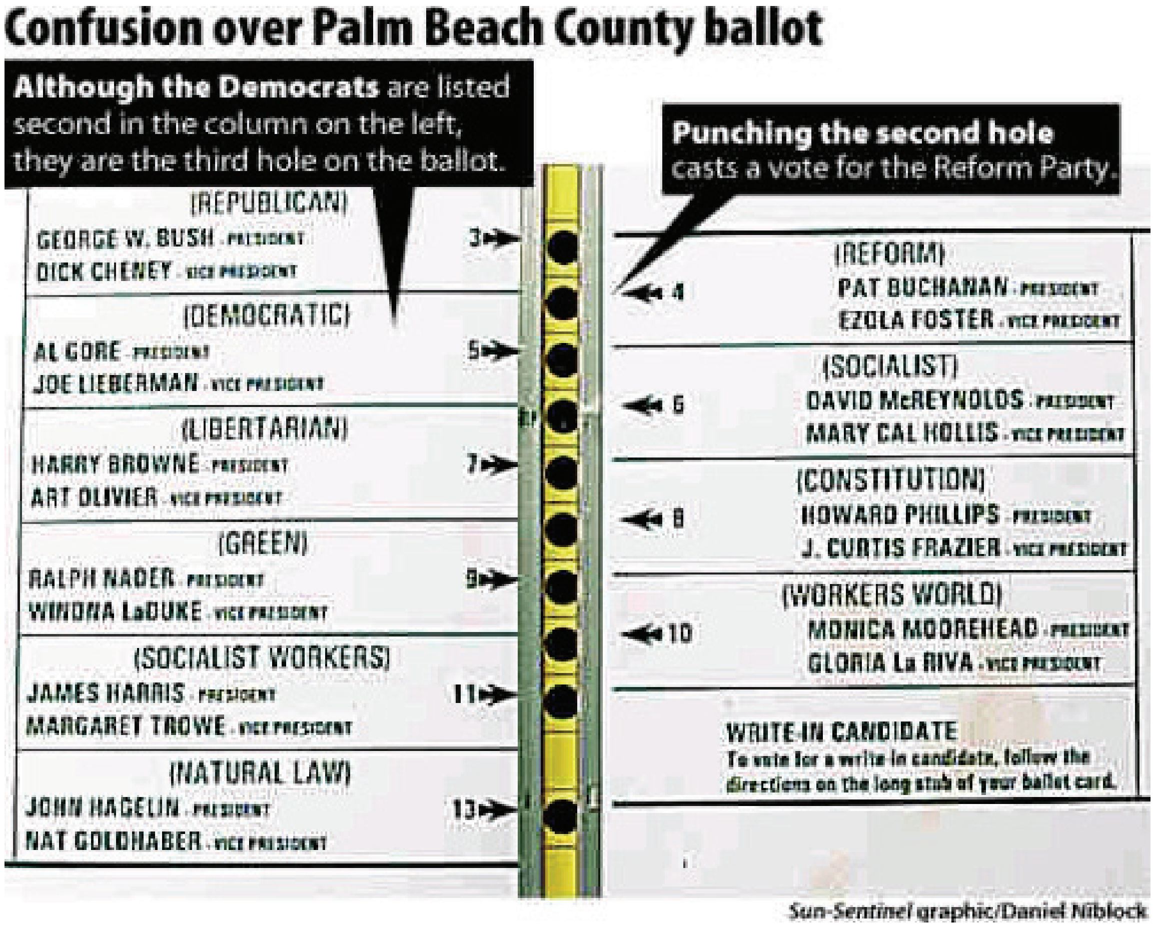


Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform Party.

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3
(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5
(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7
(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9
(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11
(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13
4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT
6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT
8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT
10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT
WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

Sun-Sentinel graphic/Daniel Niblock



Confusion over Palm Beach County ballot

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform Party.

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13

4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

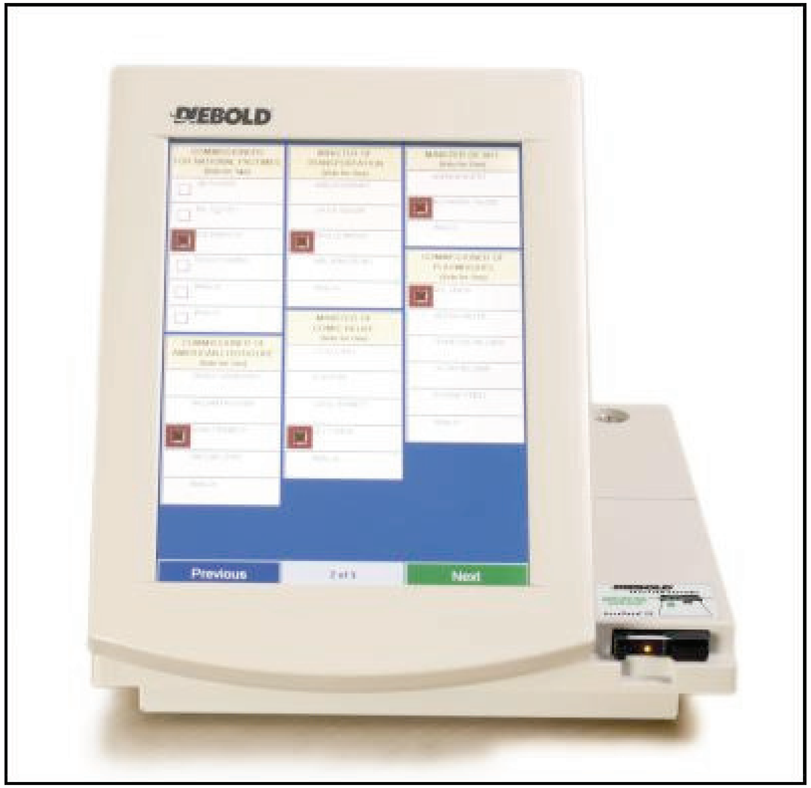
8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

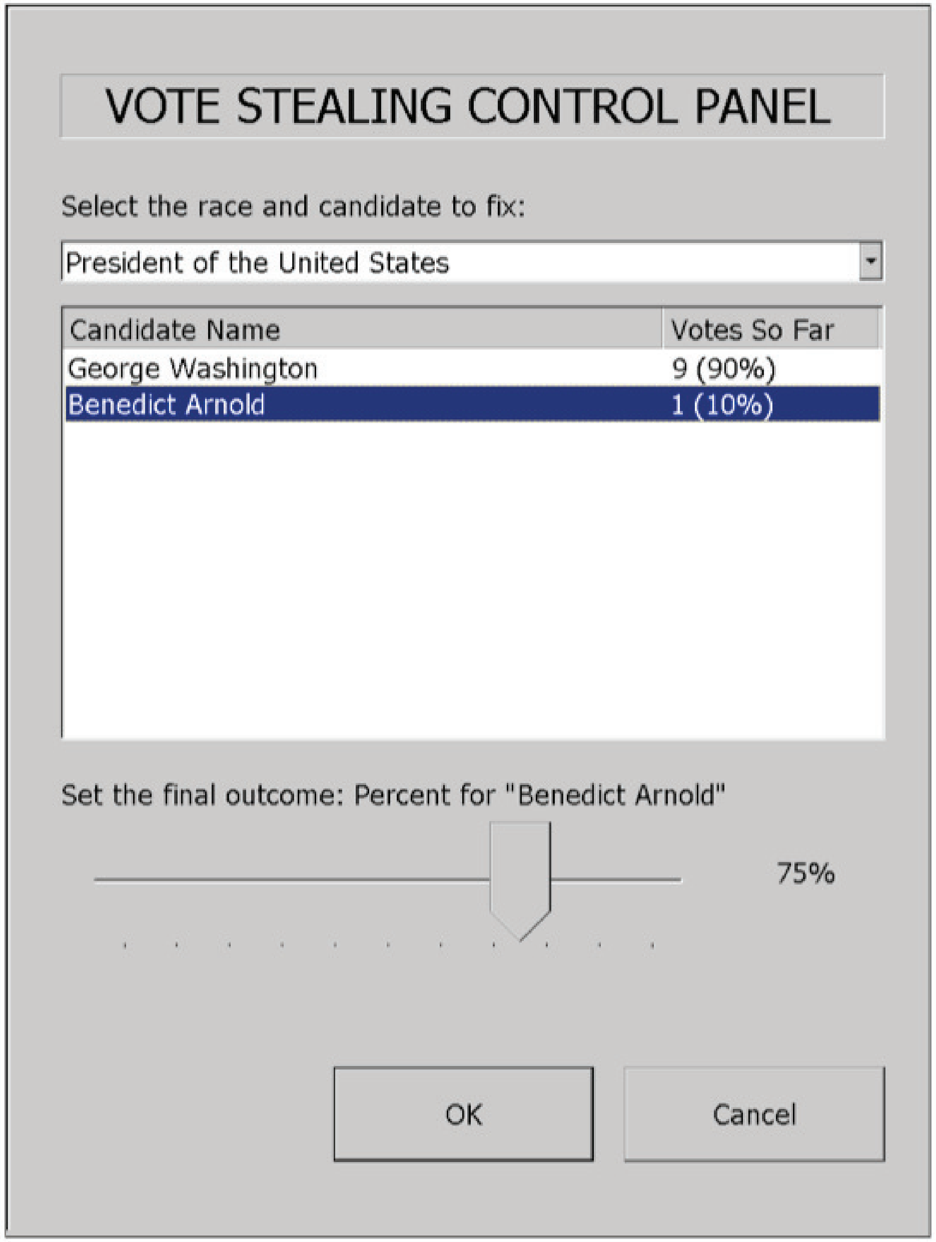
Sun-Sentinel graphic/Daniel Niblock

- 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



VOTE STEALING CONTROL PANEL

Select the race and candidate to fix:

President of the United States

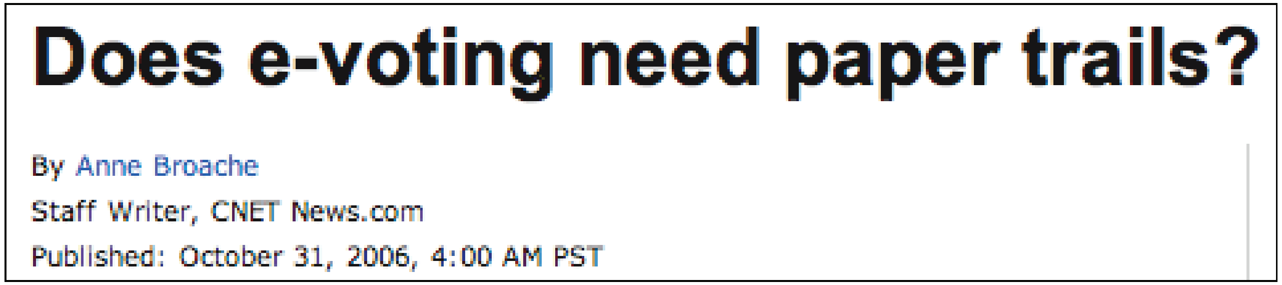
Candidate Name	Votes So Far
George Washington	9 (90%)
Benedict Arnold	1 (10%)

Set the final outcome: Percent for "Benedict Arnold"

75%

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

[FHF2006]

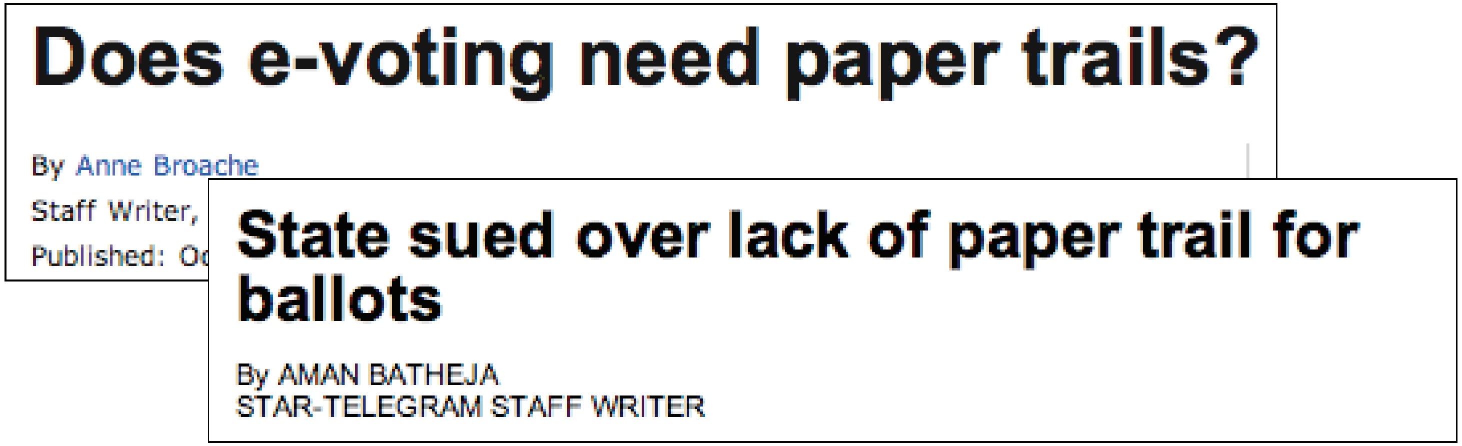


Does e-voting need paper trails?

By Anne Broache

Staff Writer, CNET News.com

Published: October 31, 2006, 4:00 AM PST



Does e-voting need paper trails?

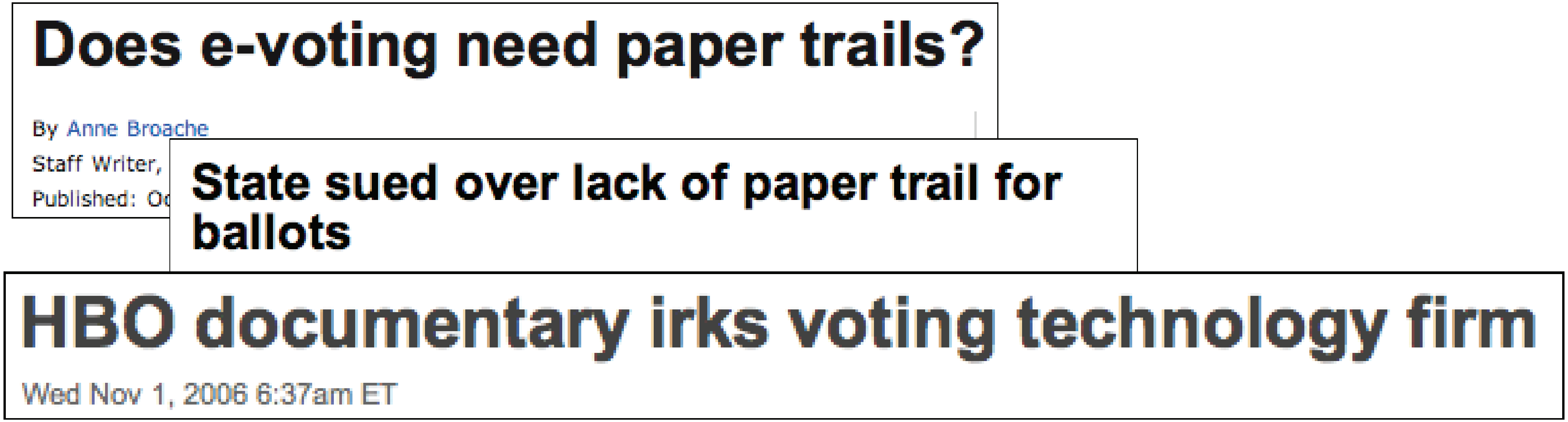
By Anne Broache

Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

By AMAN BATHEJA
STAR-TELEGRAM STAFF WRITER



Does e-voting need paper trails?

By Anne Broache

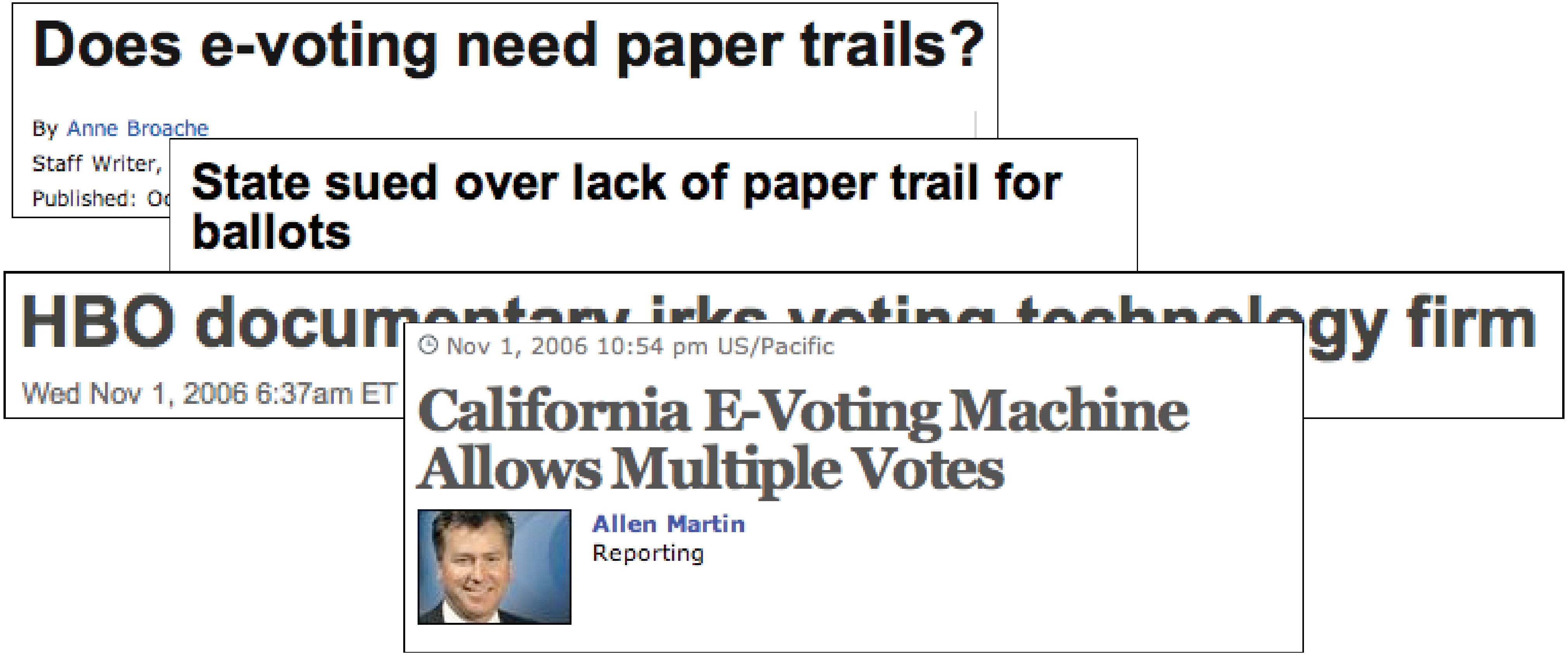
Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET



Does e-voting need paper trails?

By Anne Broache

Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

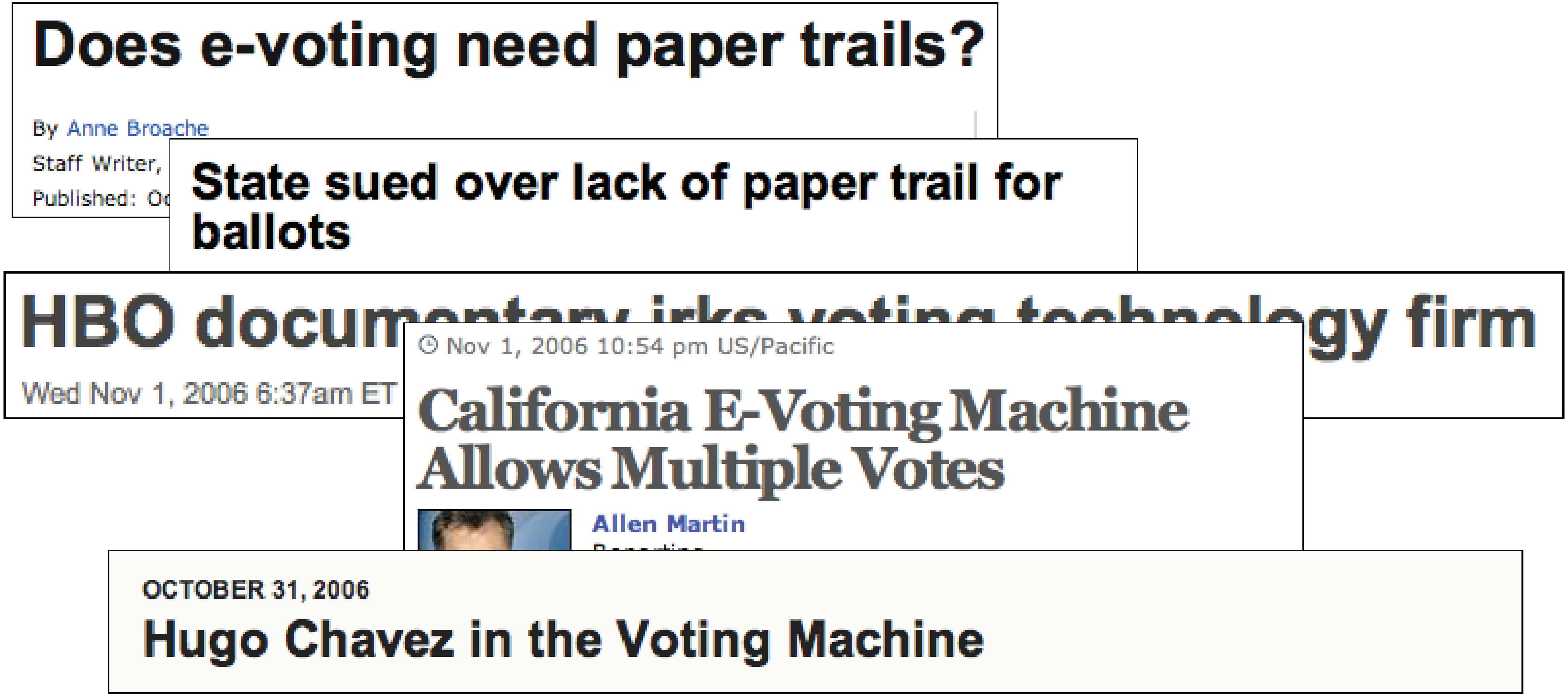
Wed Nov 1, 2006 6:37am ET

Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin

Reporting



Does e-voting need paper trails?

By Anne Broache

Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET

Nov 1, 2006 10:54 pm US/Pacific

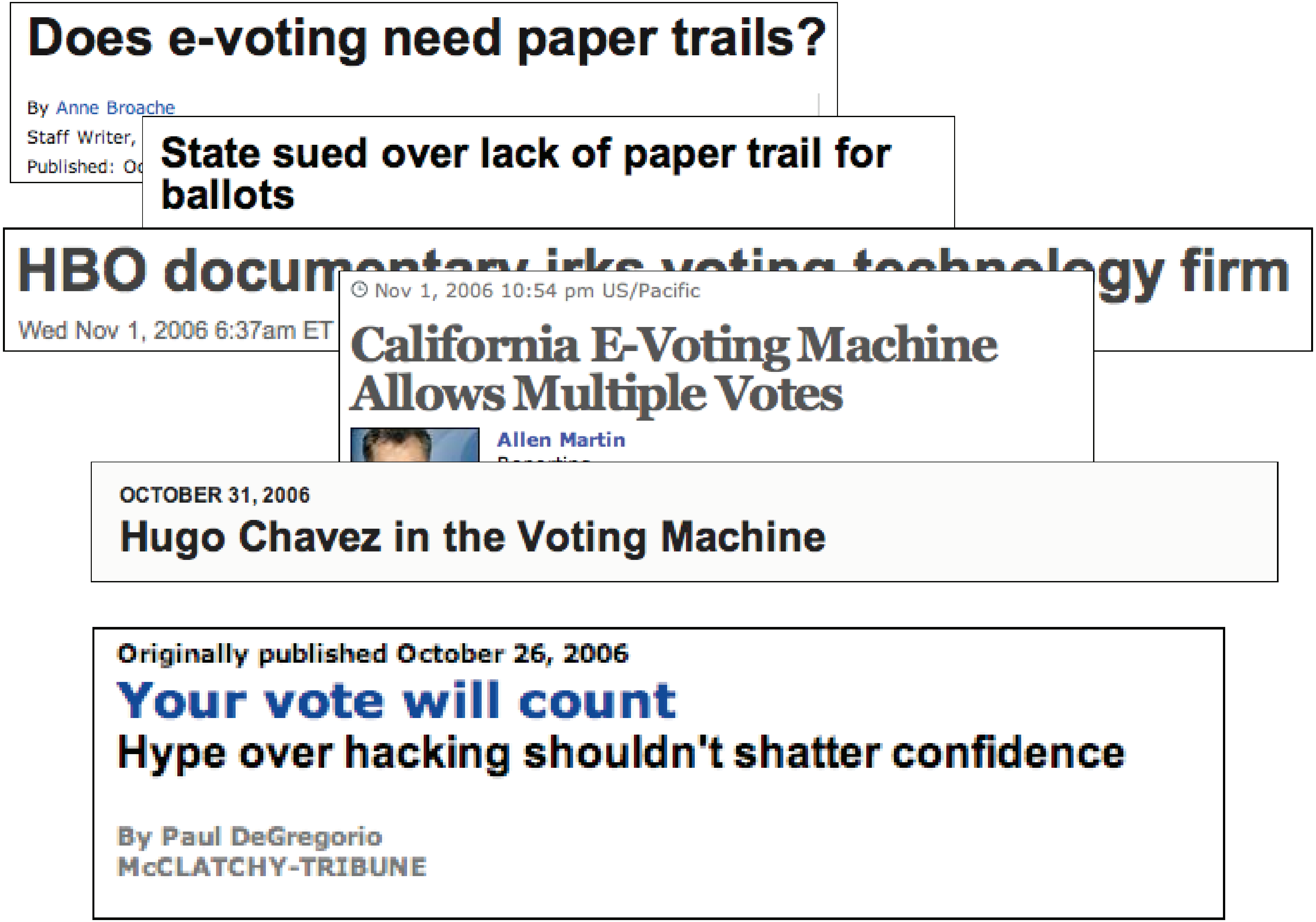
California E-Voting Machine Allows Multiple Votes

Allen Martin

Reporting

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine



Does e-voting need paper trails?

By Anne Broache

Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET

Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine

Originally published October 26, 2006

Your vote will count

Hype over hacking shouldn't shatter confidence

By Paul DeGregorio
McCLATCHY-TRIBUNE

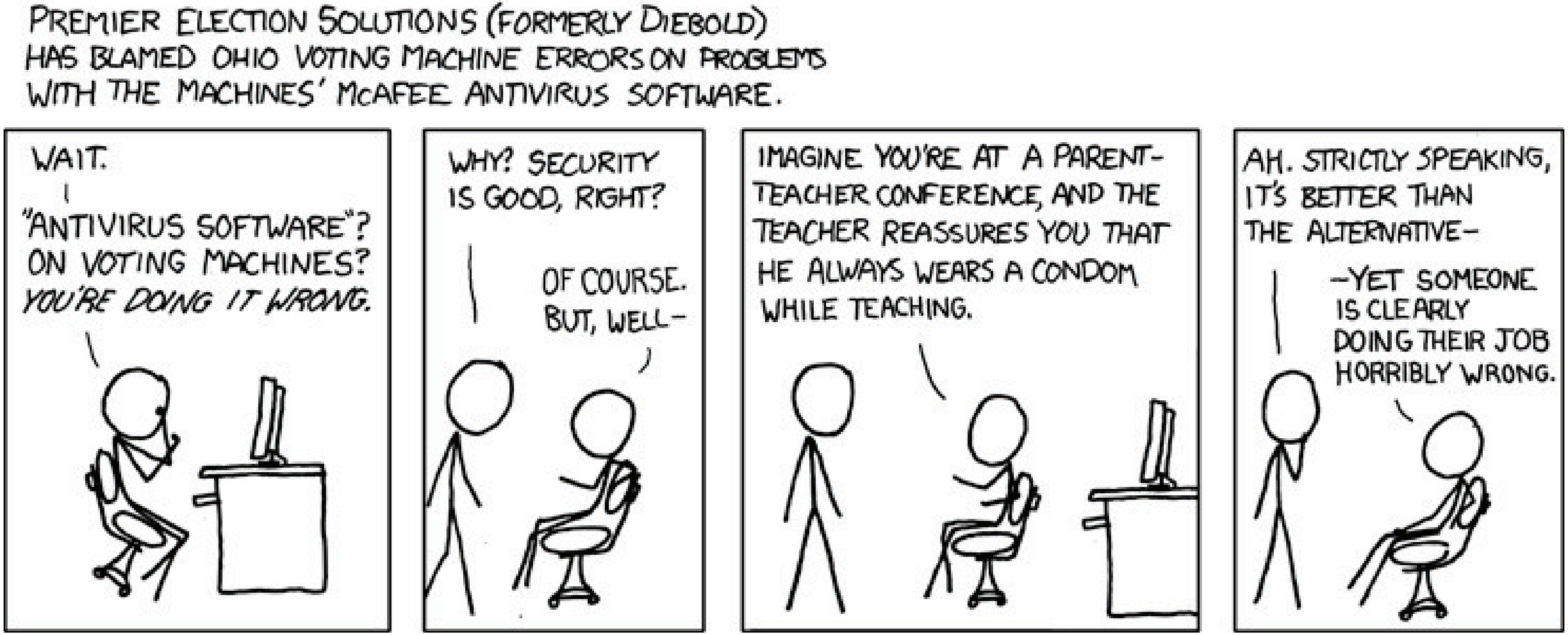
- New Mexico (March 2006)
- California (August 2007)
- Florida (December 2007)
- Ohio (January 2008)
- Iowa (March 2008)
- ...

- 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


PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD) HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.
WAIT.
"ANTIVIRUS SOFTWARE"? ON VOTING MACHINES? *YOU'RE DOING IT WRONG.*
WHY? SECURITY IS GOOD, RIGHT?
OF COURSE. BUT, WELL–
IMAGINE YOU'RE AT A PARENT-TEACHER CONFERENCE, AND THE TEACHER REASSURES YOU THAT HE ALWAYS WEARS A CONDOM WHILE TEACHING.
AH. STRICTLY SPEAKING, IT'S BETTER THAN THE ALTERNATIVE–
–YET SOMEONE IS CLEARLY DOING THEIR JOB HORRIBLY WRONG.

http://xkcd.com/463/

What does Everbody Want?

- Simple and reliable system
- Voter secrecy
- Quick count

- And in addition: transparency (open audit).

What is Transparency?

Anyone can verify that:

- their vote was **cast as intended**
- the votes were **count as cast**

And, in case of a problem, can recount and obtain the correct result (e.g. paper trail)

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

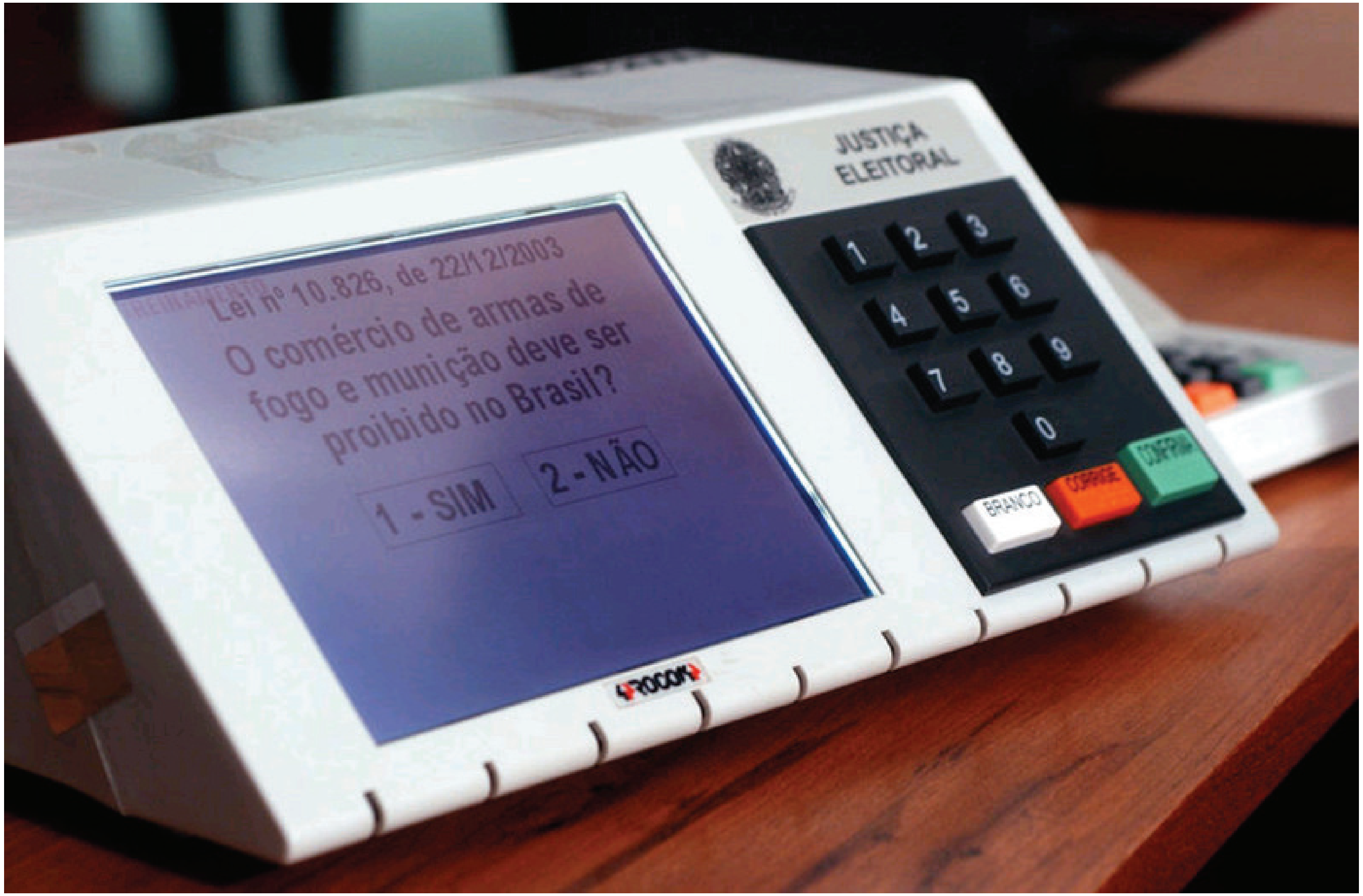
Software Independence [Rivest, Wack'06]

"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"

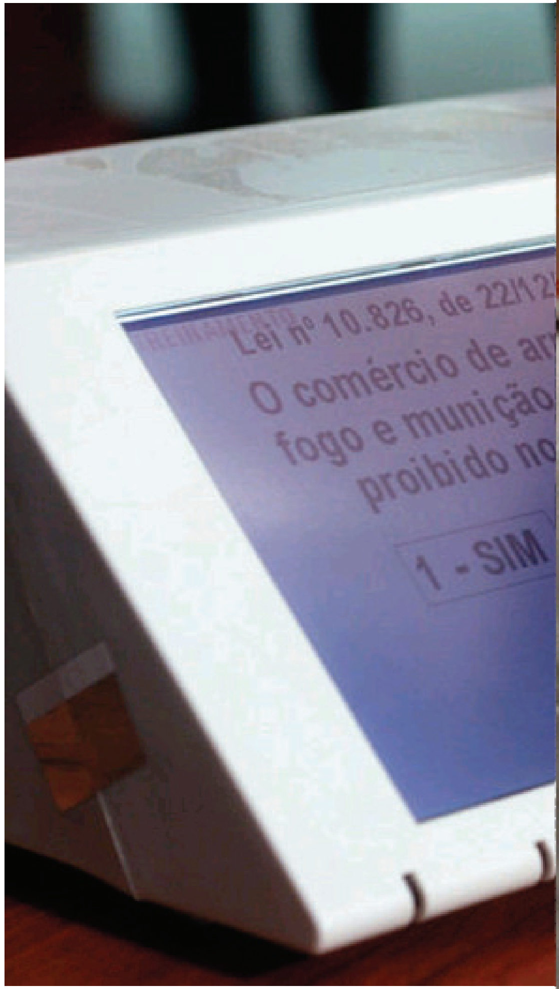
Examples

Examples

Non-examples


JUSTIÇA ELEITORAL
TREINAMENTO
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

Non-examples



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 in Oct ’08 election.
- Aug’08 - Speedy 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

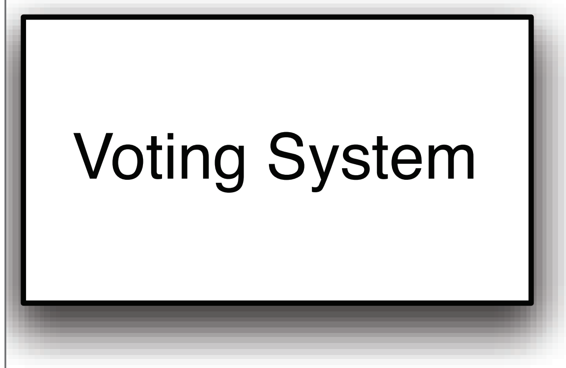
“The People have spoken....
the bastards!”

Dick Tuck
1966 Concession Speech

Provide enough evidence to convince the loser.

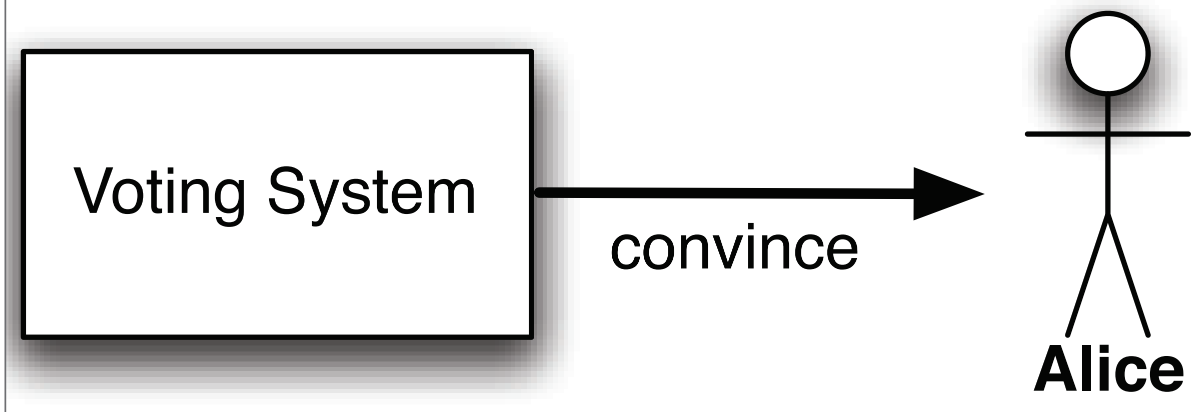
Secret Ballot *vs.* Verifiability

Secret Ballot *vs.* Verifiability

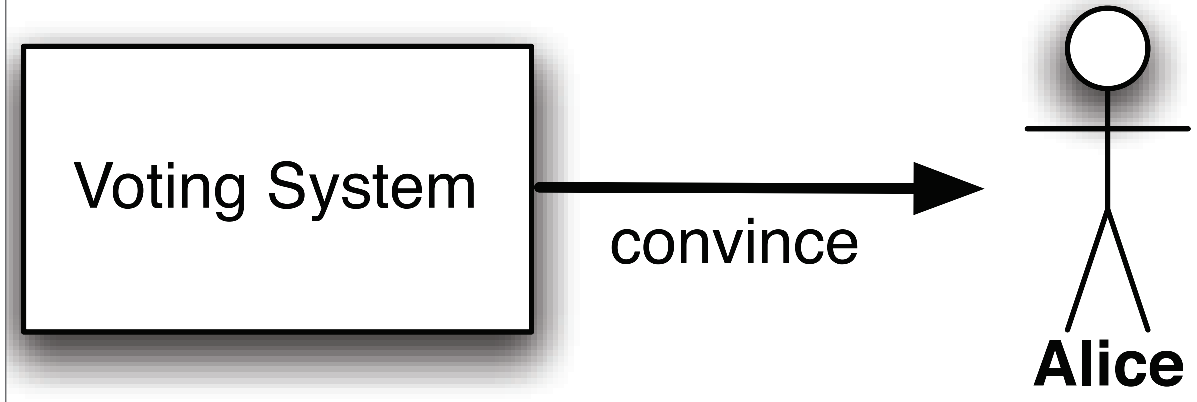


Voting System

Secret Ballot *vs.* Verifiability



Secret Ballot *vs.* Verifiability



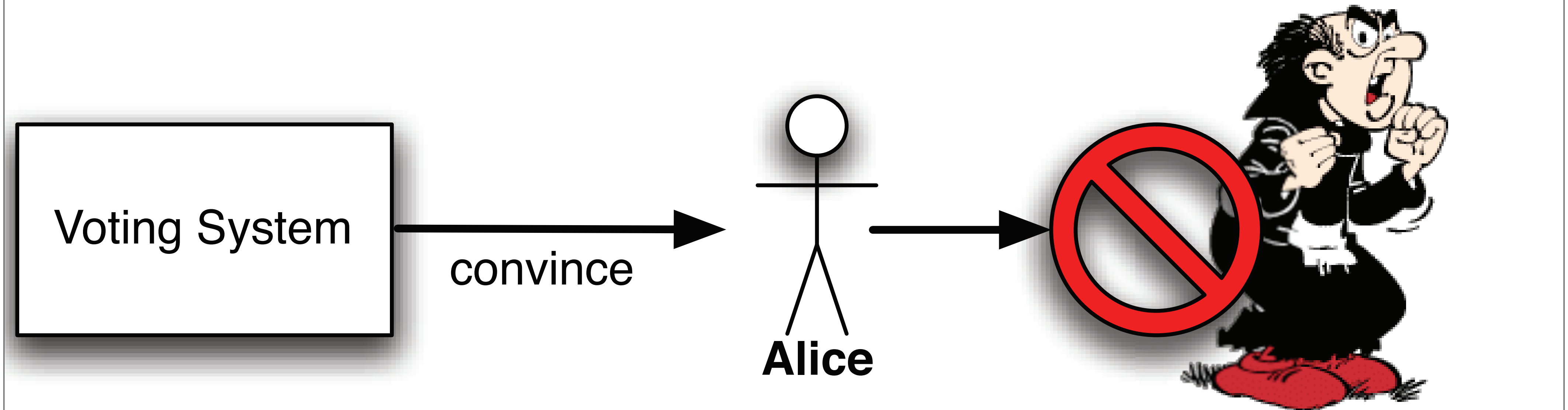
Voting System

convince

Alice

Carl the Coercer

Secret Ballot *vs.* Verifiability



Voting System

convince

Alice

Carl the Coercer

Desired Properties

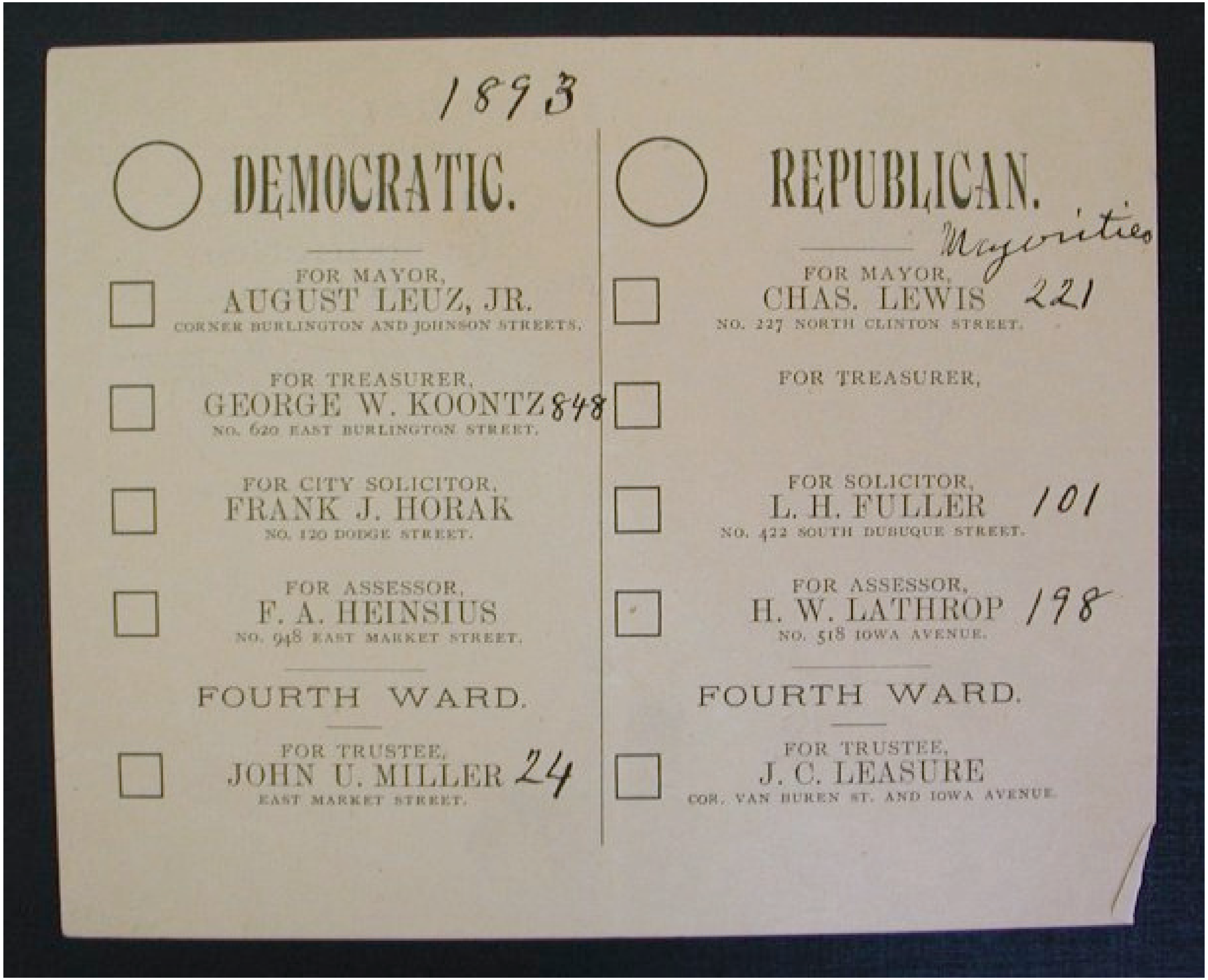
(1)**Alice** verifies **her vote**.

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

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

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

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 Breakfast Election

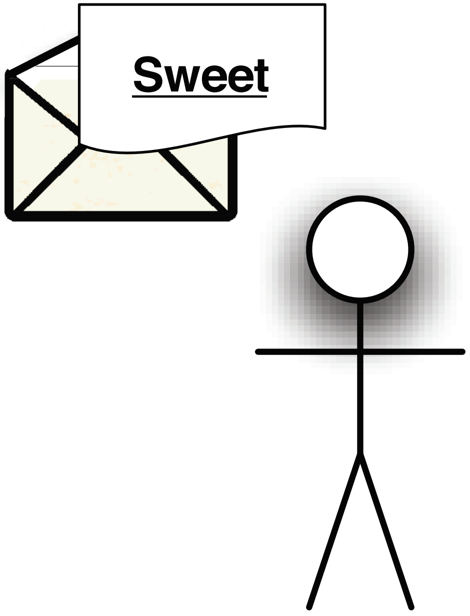
Salty

Sweet

http://en.wikipedia.org/wiki/Image:FoodOmelete.jpg

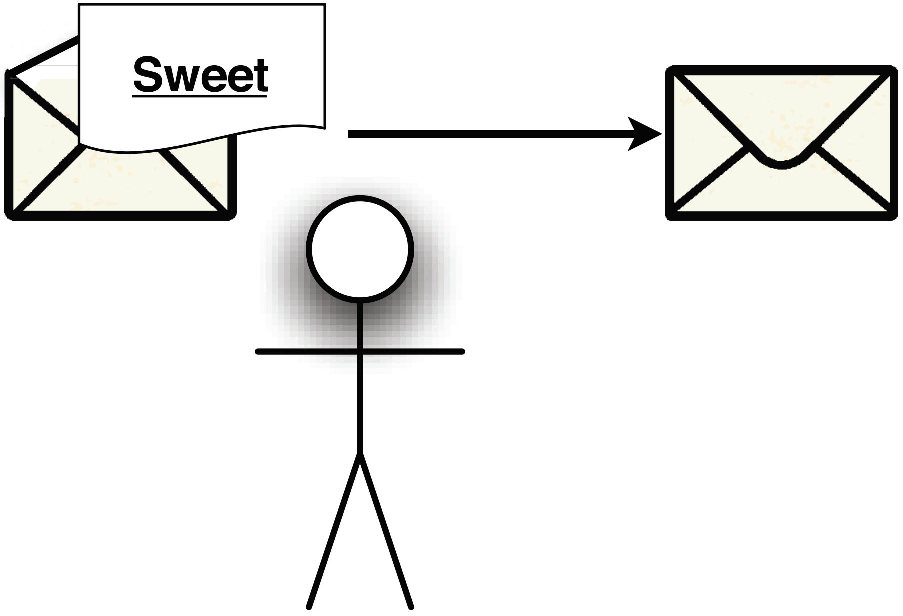
http://www.flickr.com/photos/35034346243@N01/91524057/

The Ballot Handoff



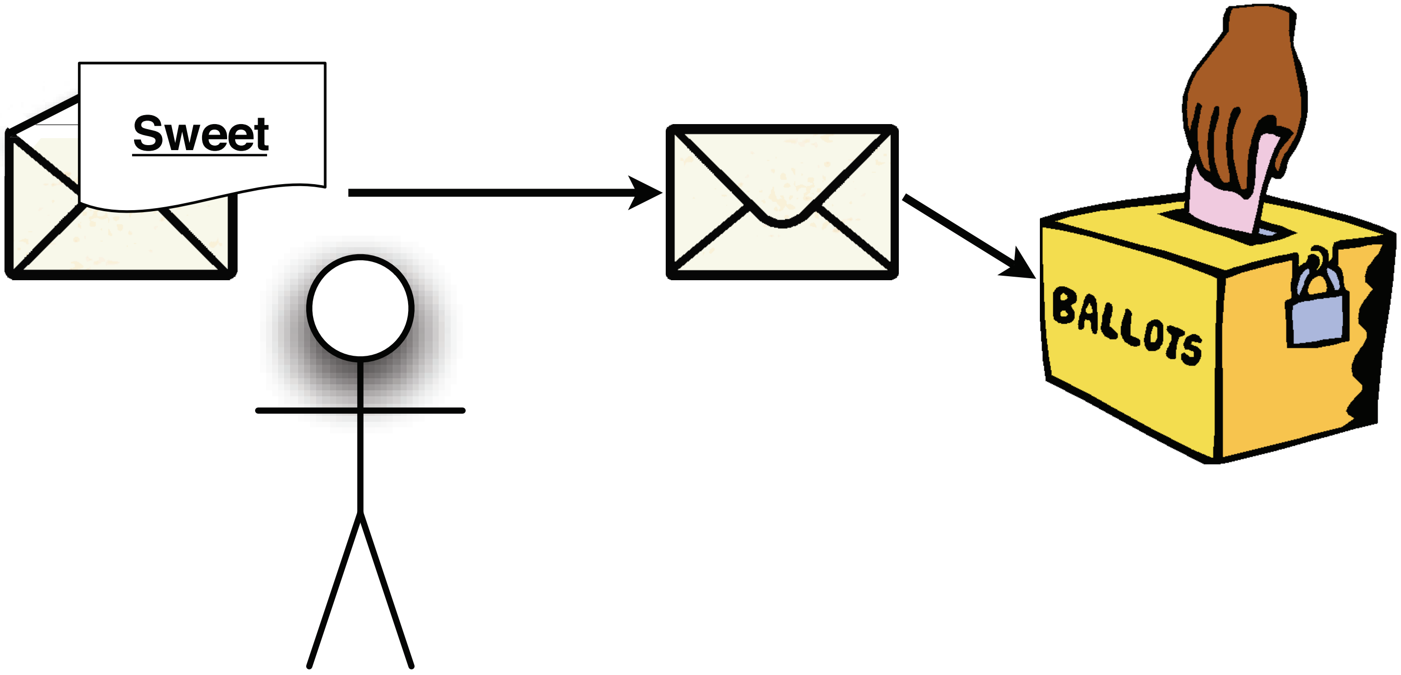
Alice the Voter

The Ballot Handoff



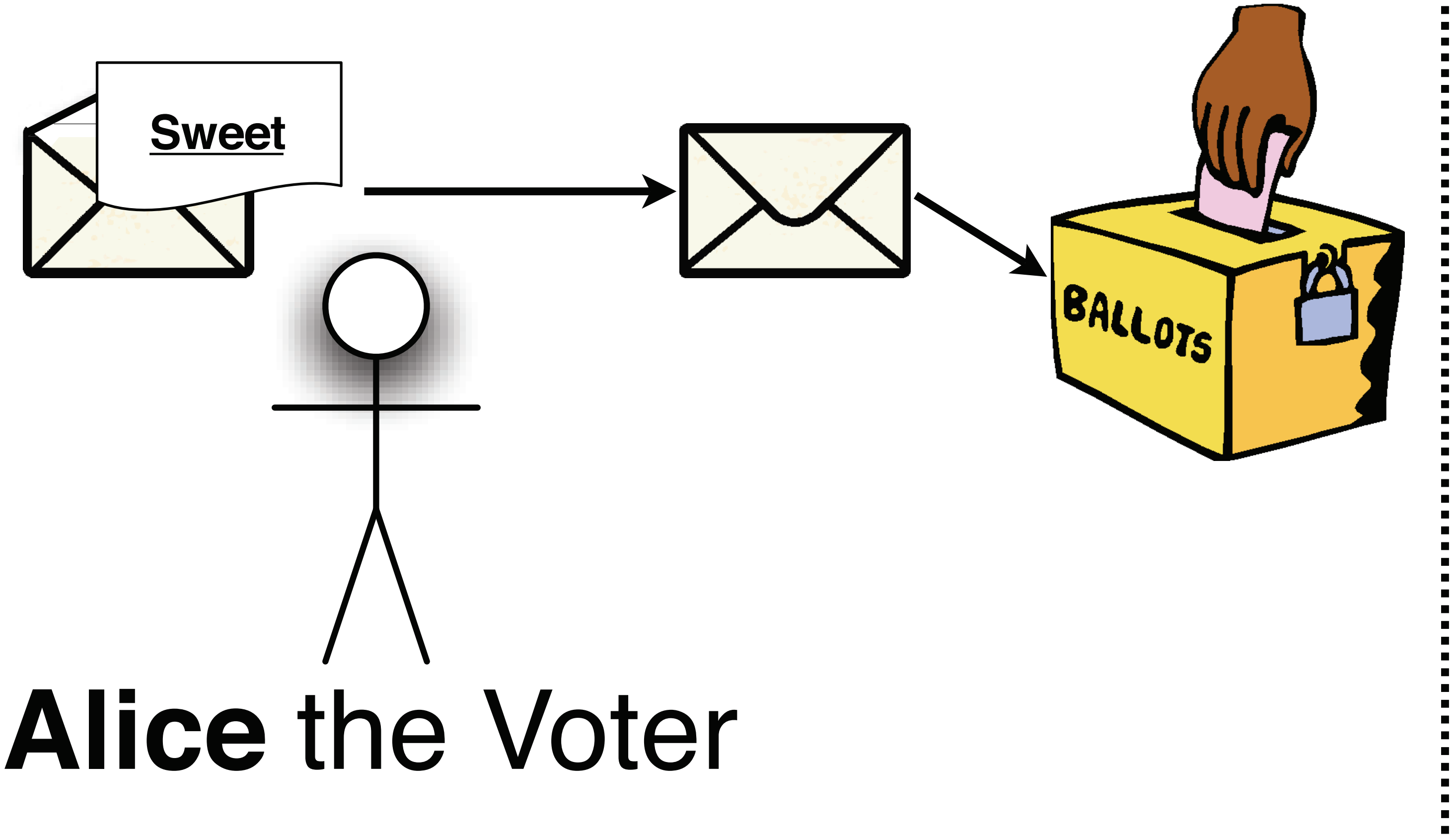
Alice the Voter

The Ballot Handoff



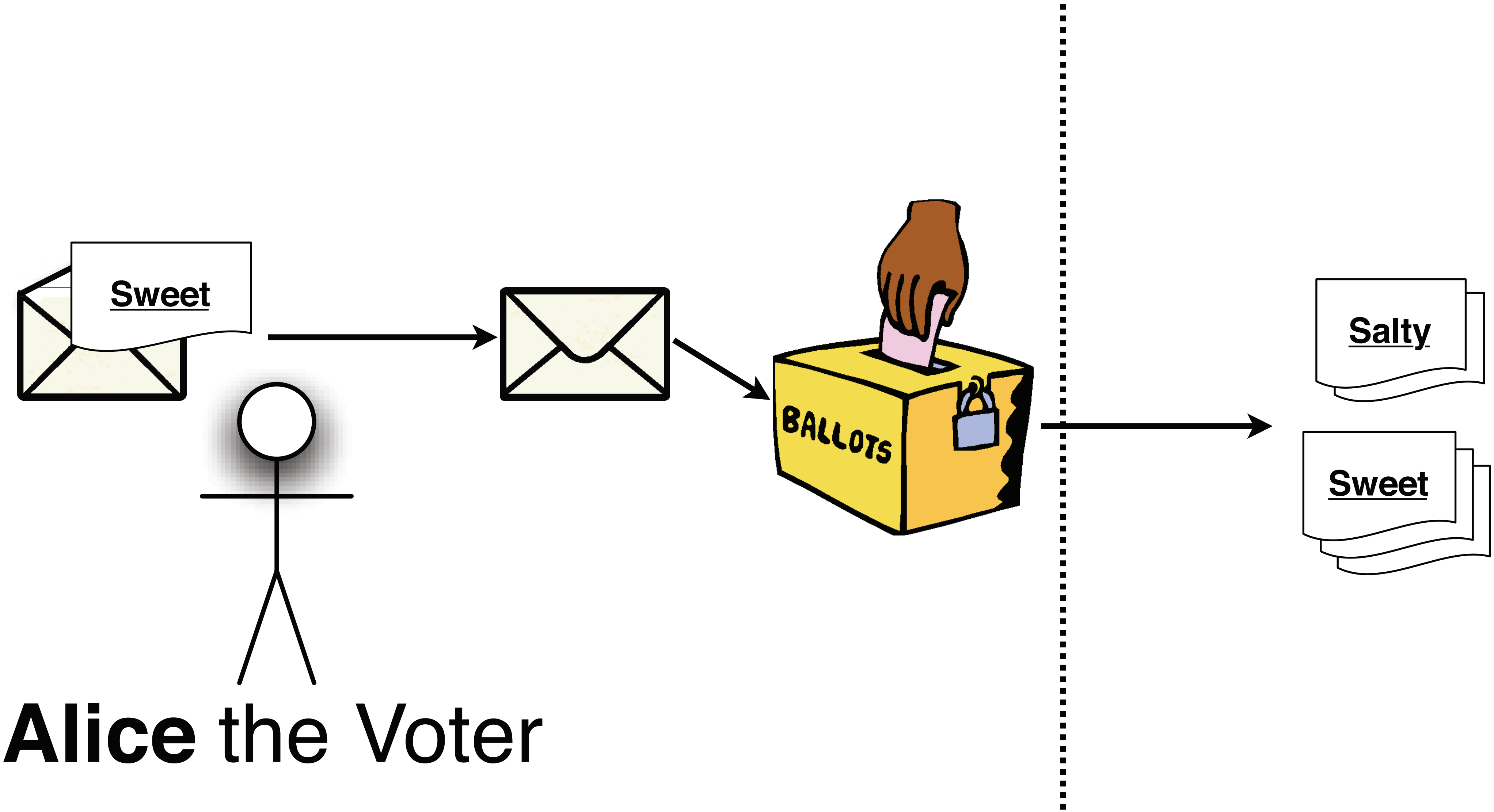
Alice the Voter

The Ballot Handoff



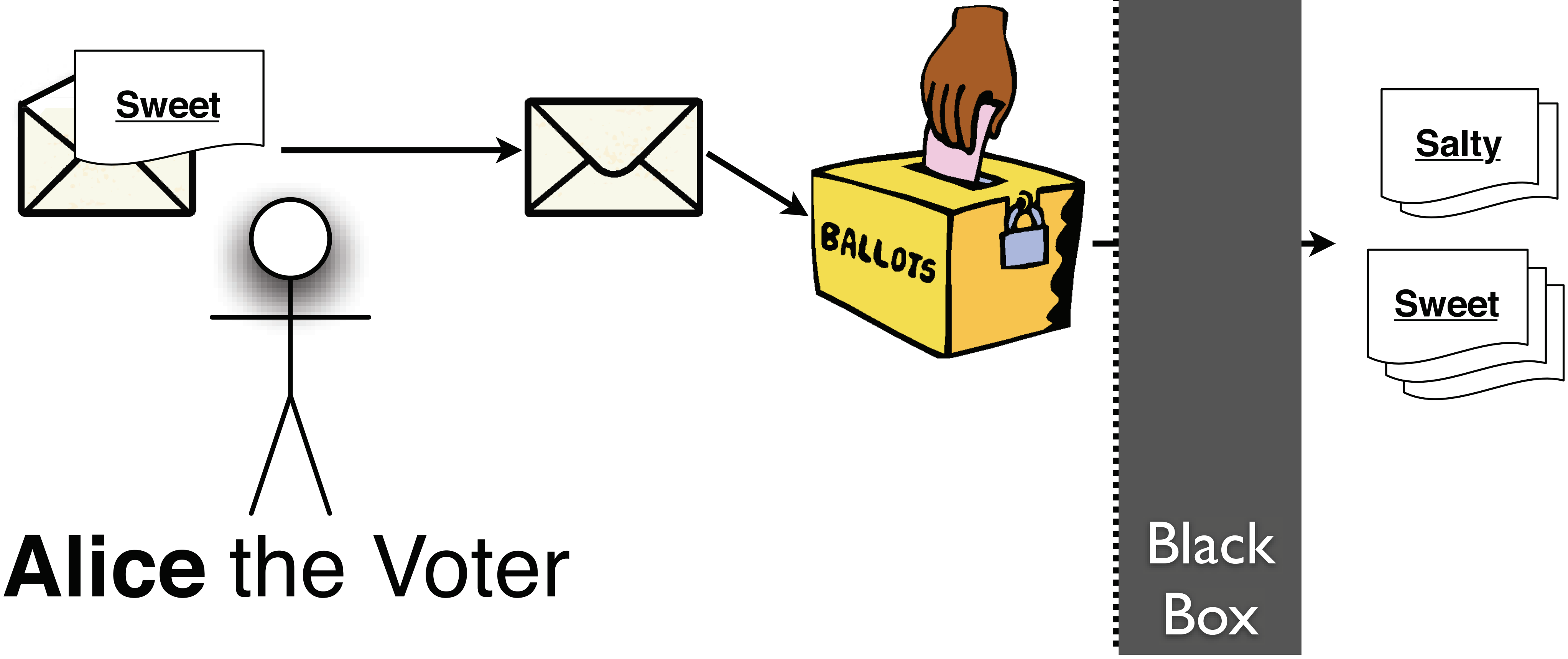
Alice the Voter

The Ballot Handoff



Alice the Voter

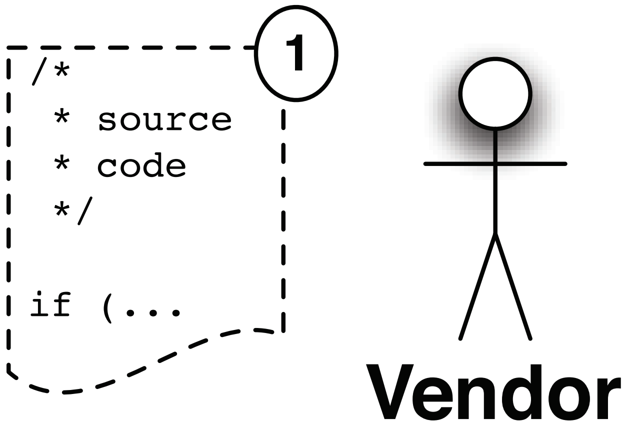
The Ballot Handoff



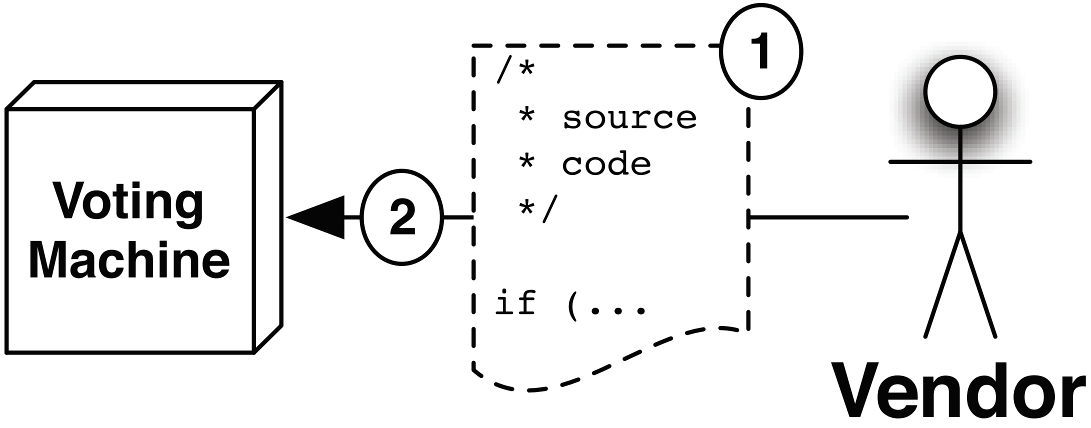
Alice the Voter

Chain of Custody

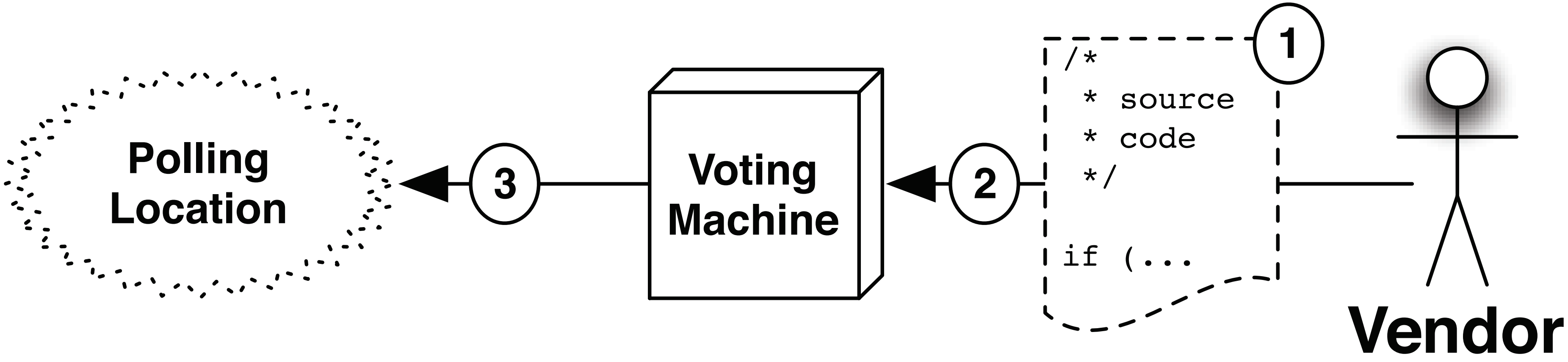
Chain of Custody



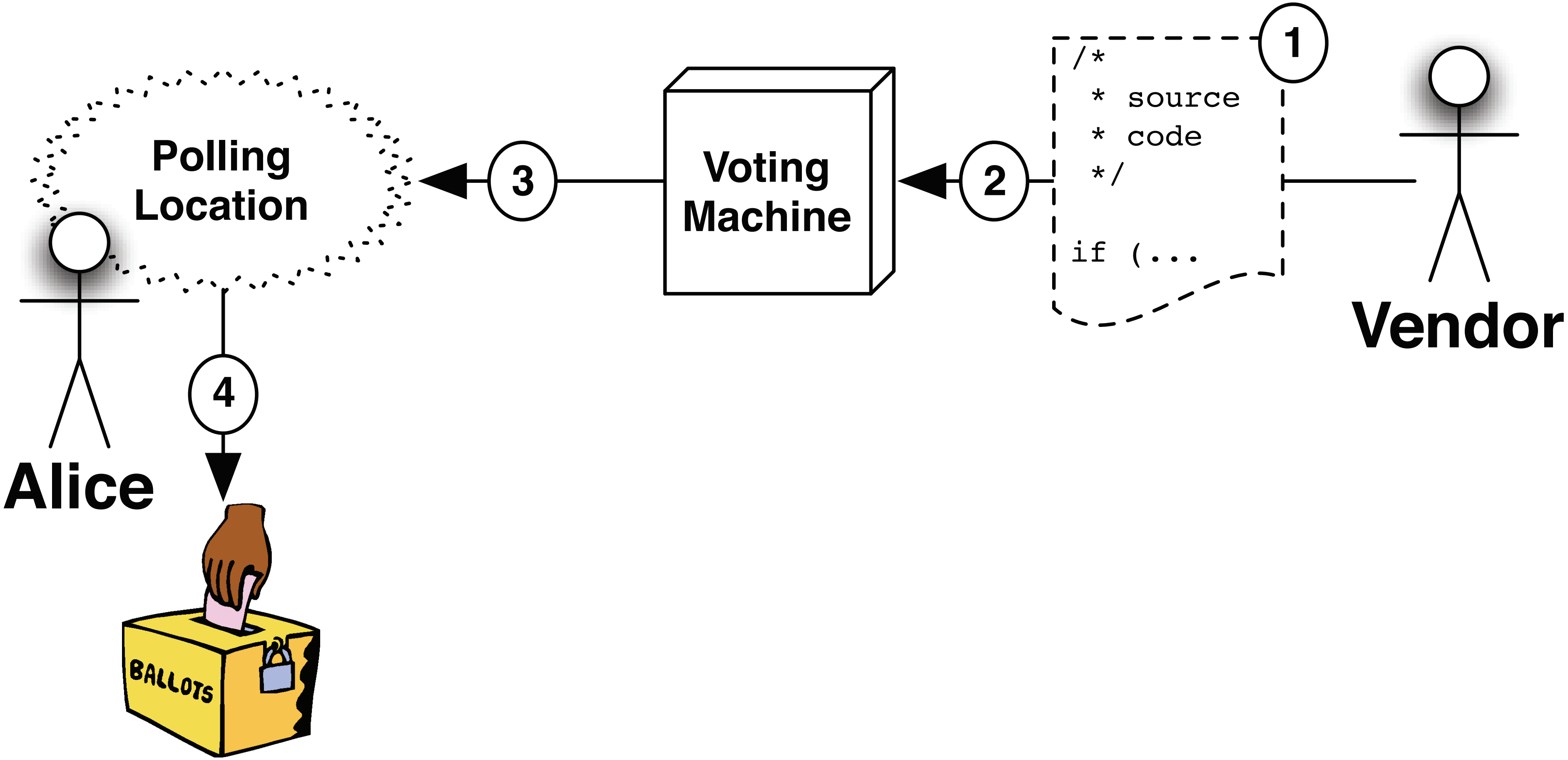
Chain of Custody



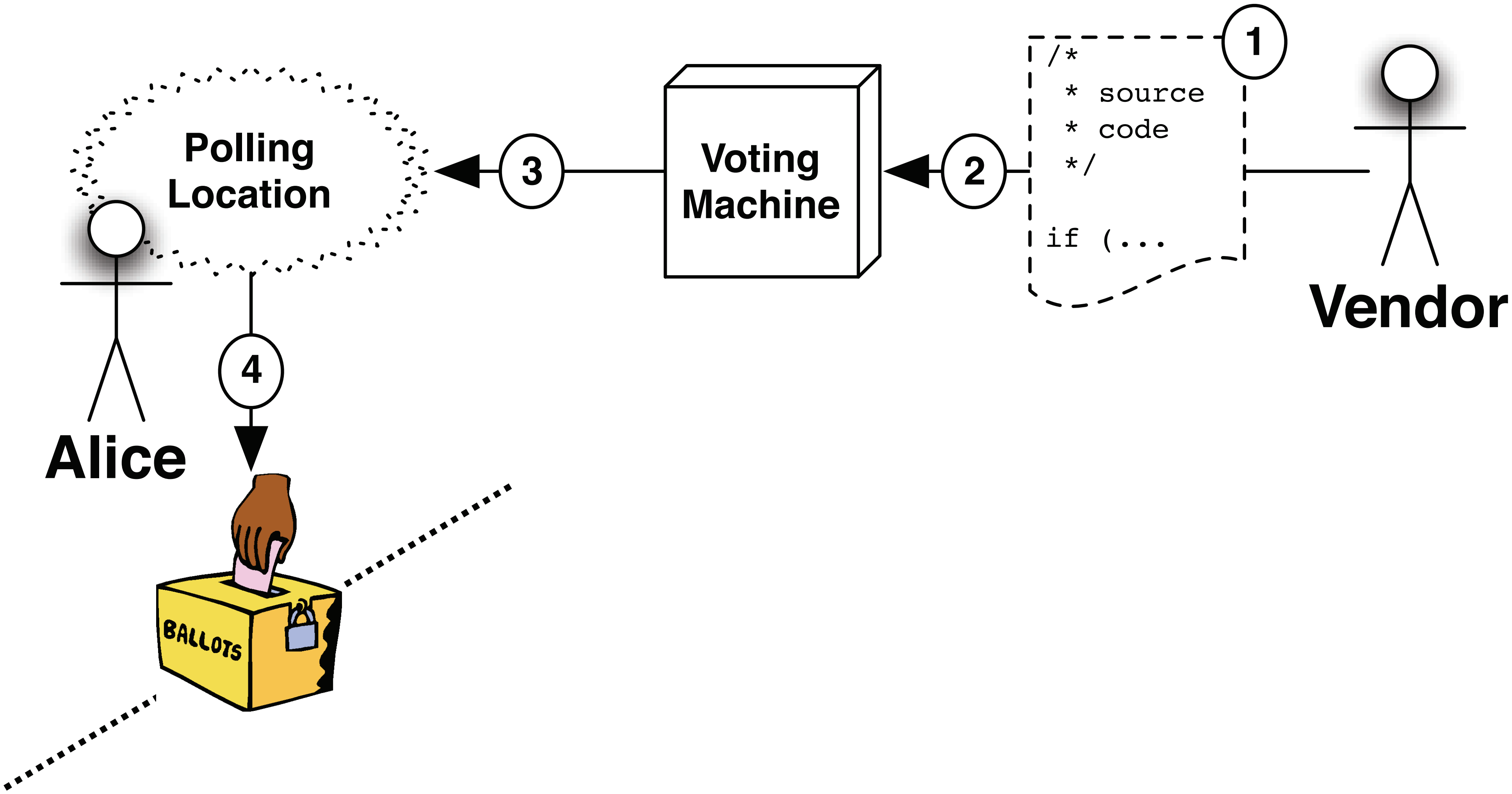
Chain of Custody



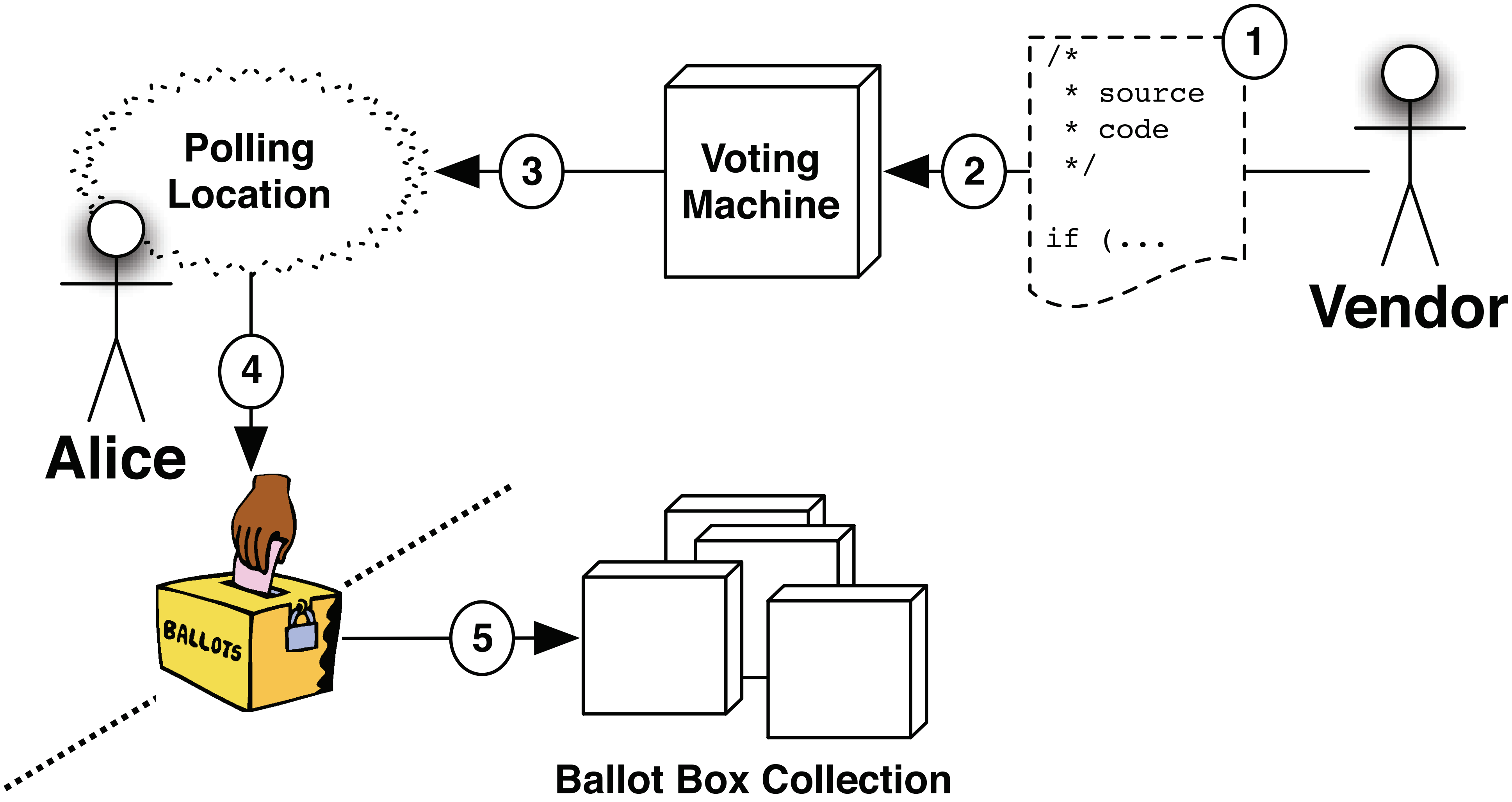
Chain of Custody



Chain of Custody



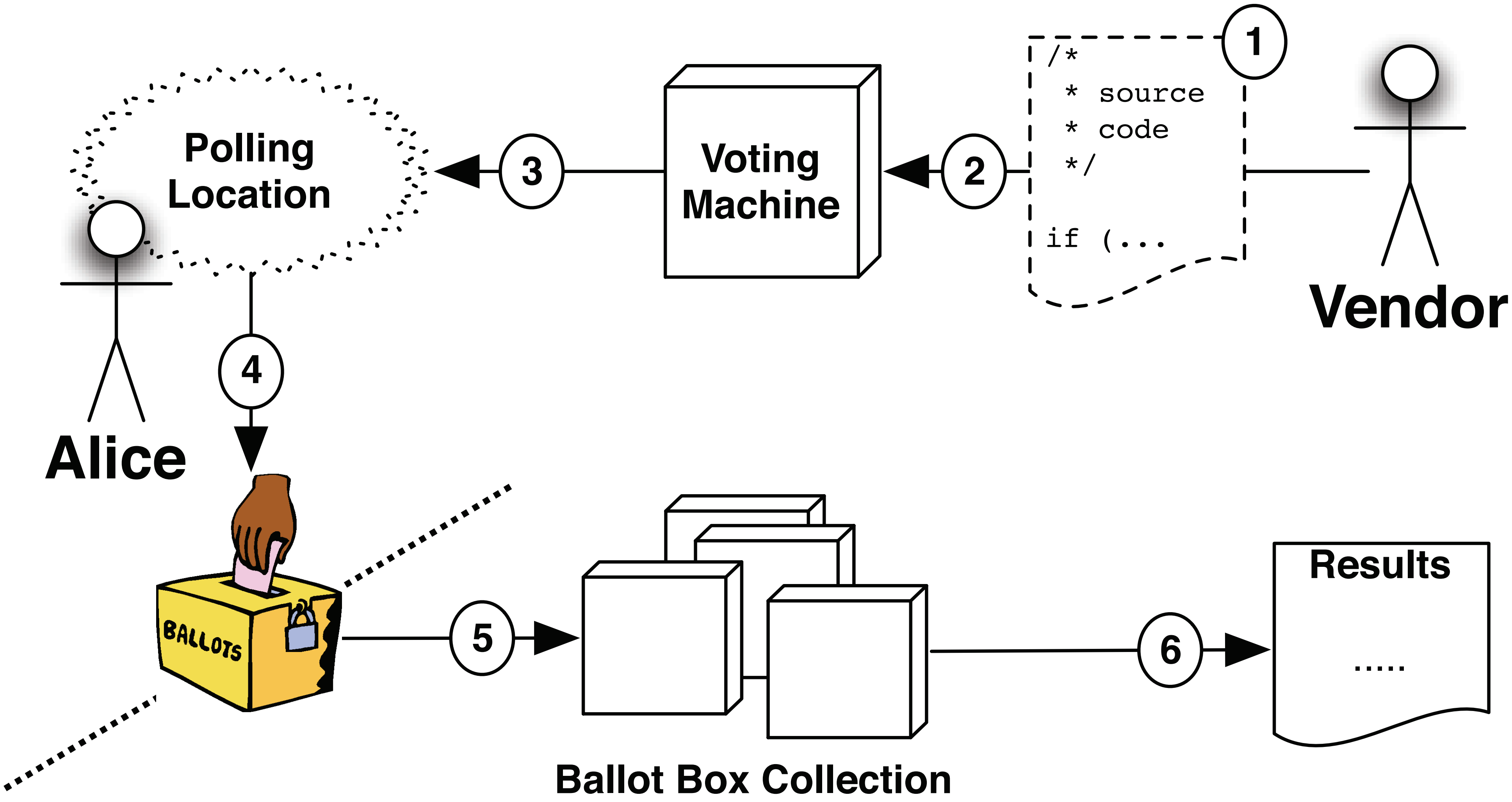
Chain of Custody



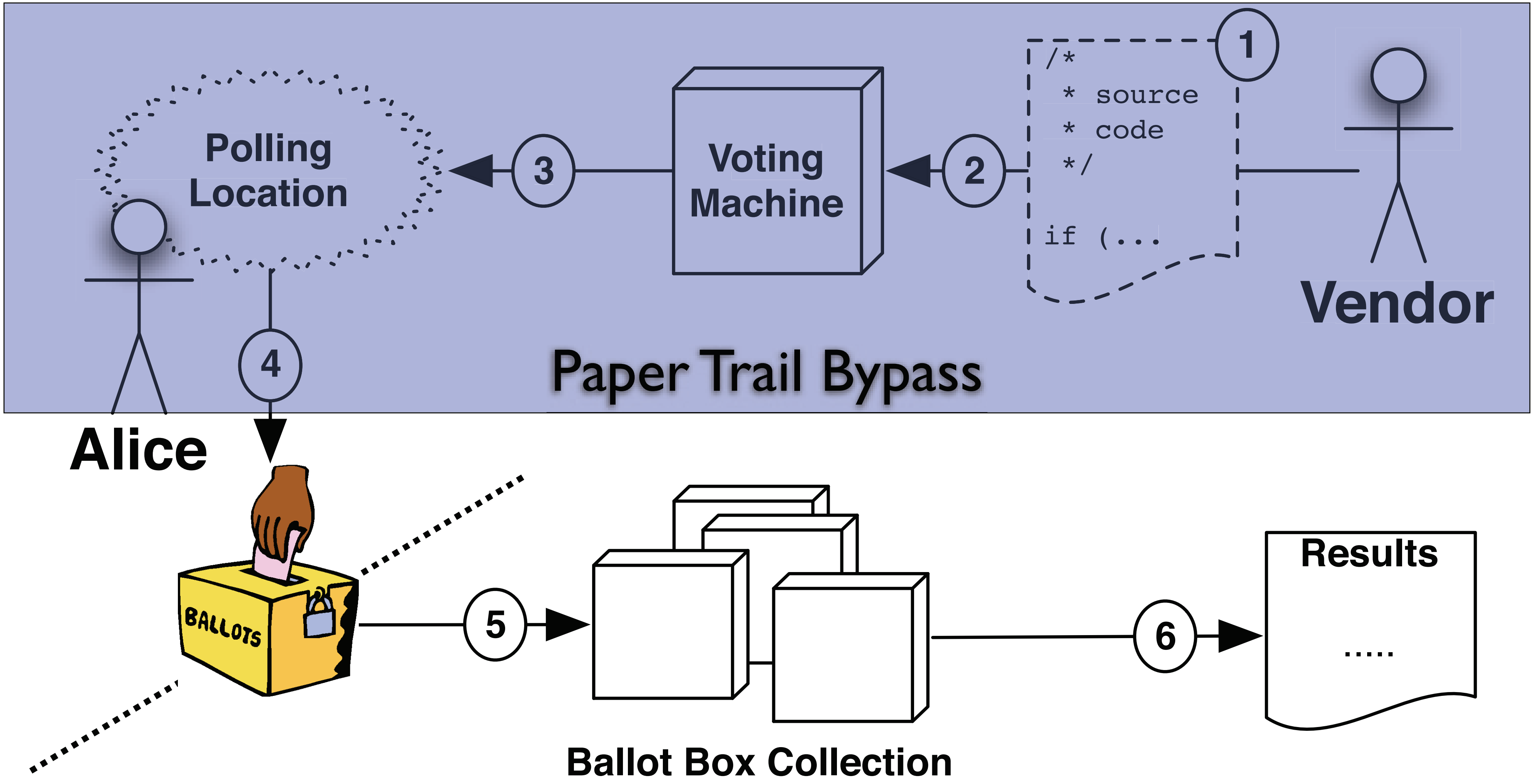
```
/*
 * source
 * code
 */

if (...
```

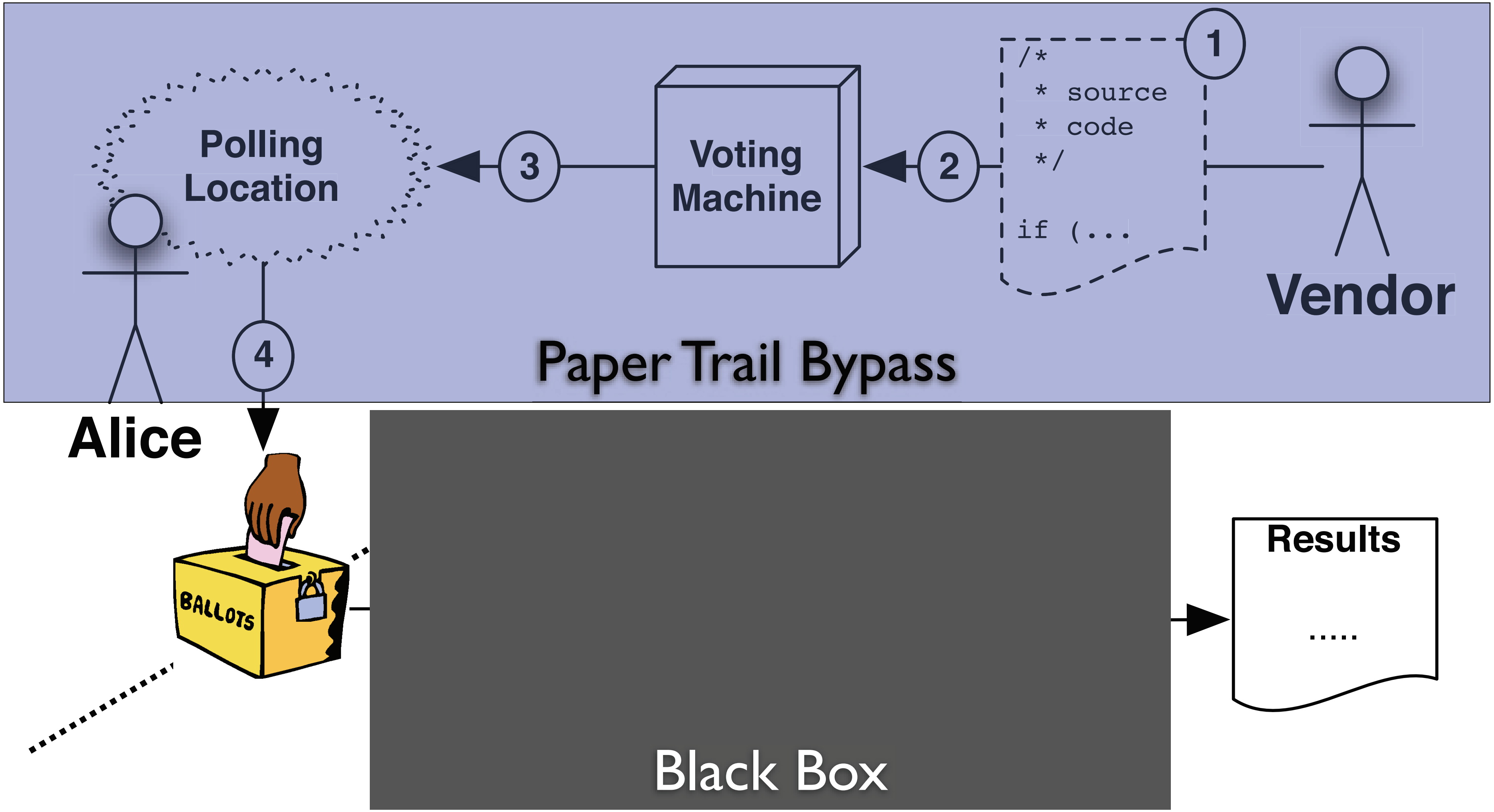
Chain of Custody



Chain of Custody



Chain of Custody



Polling Location

Voting Machine

```
/*
 * source
 * code
 */

if (...
```

1

2

3

4

Vendor

Alice

Paper Trail Bypass

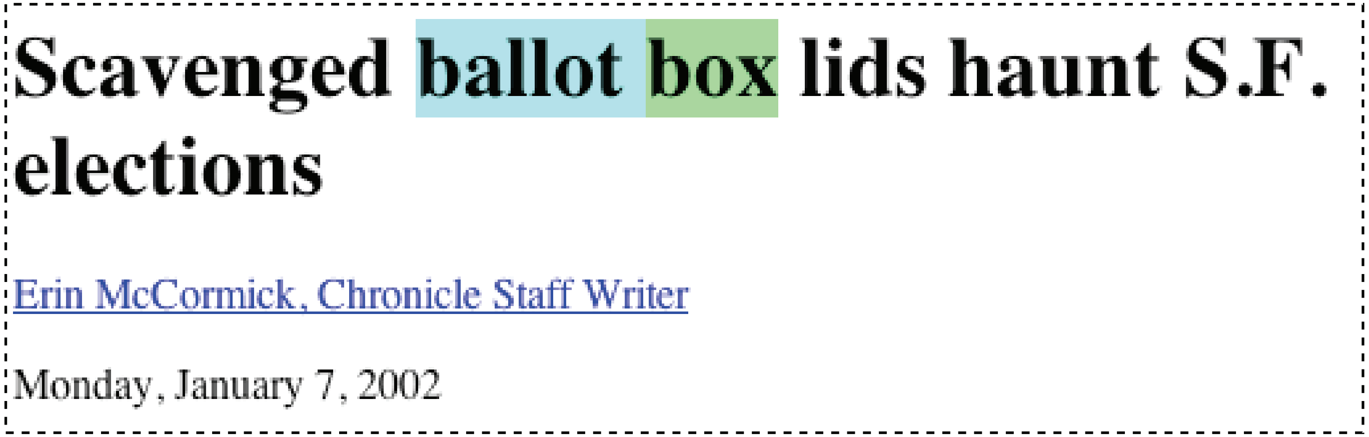
Black Box

Results

.....

The Cost of Secrecy

The Cost of Secrecy

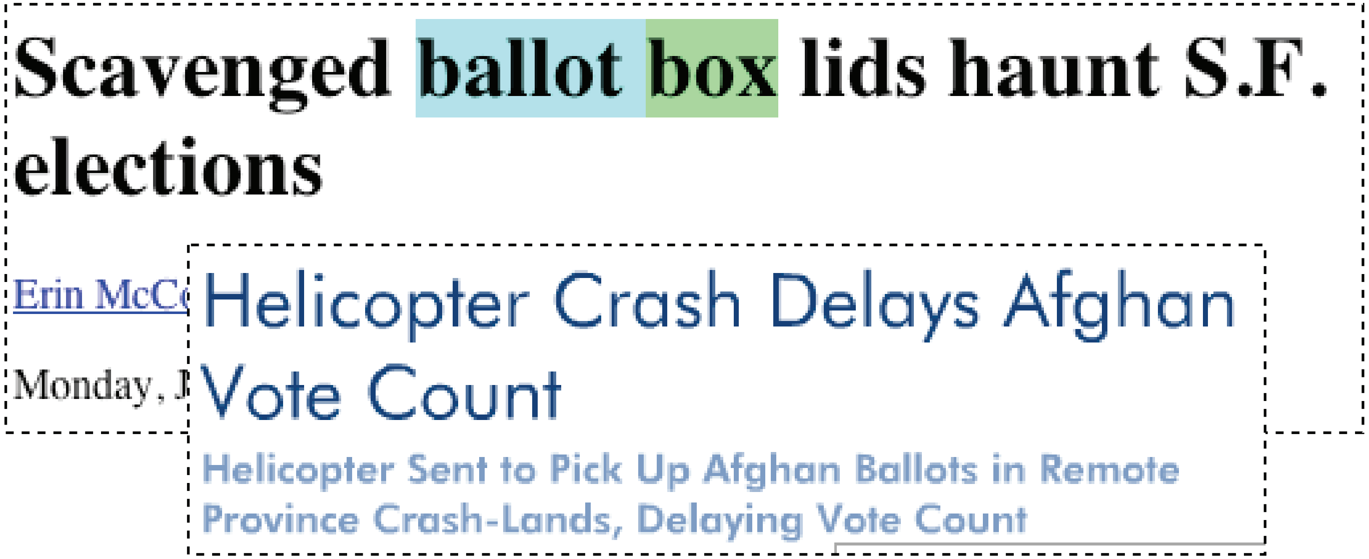


Scavenged ballot box lids haunt S.F. elections

Erin McCormick, Chronicle Staff Writer

Monday, January 7, 2002

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

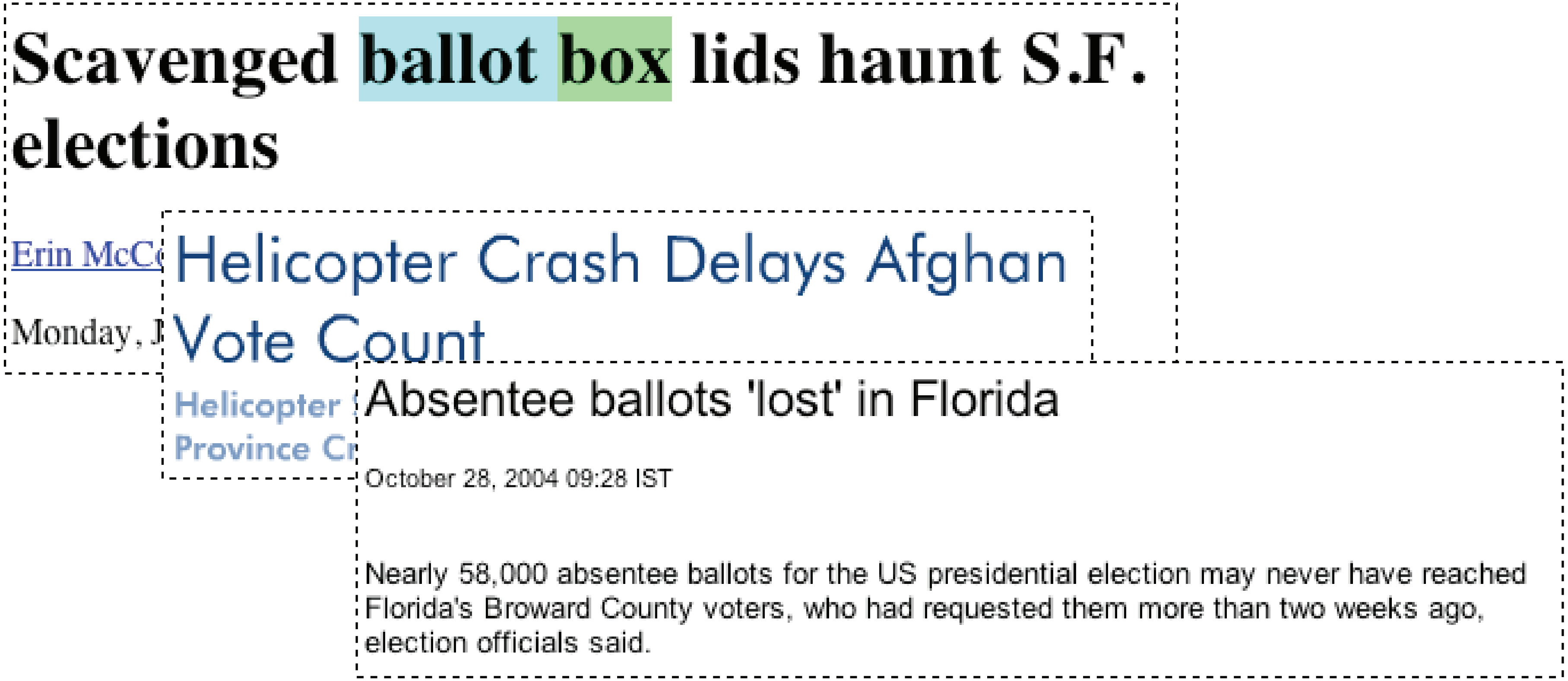
Erin McC

Monday,

Helicopter Crash Delays Afghan Vote Count

Helicopter Sent to Pick Up Afghan Ballots in Remote Province Crash-Lands, Delaying Vote Count

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, J

Helicopter Crash Delays Afghan Vote Count

Helicopter

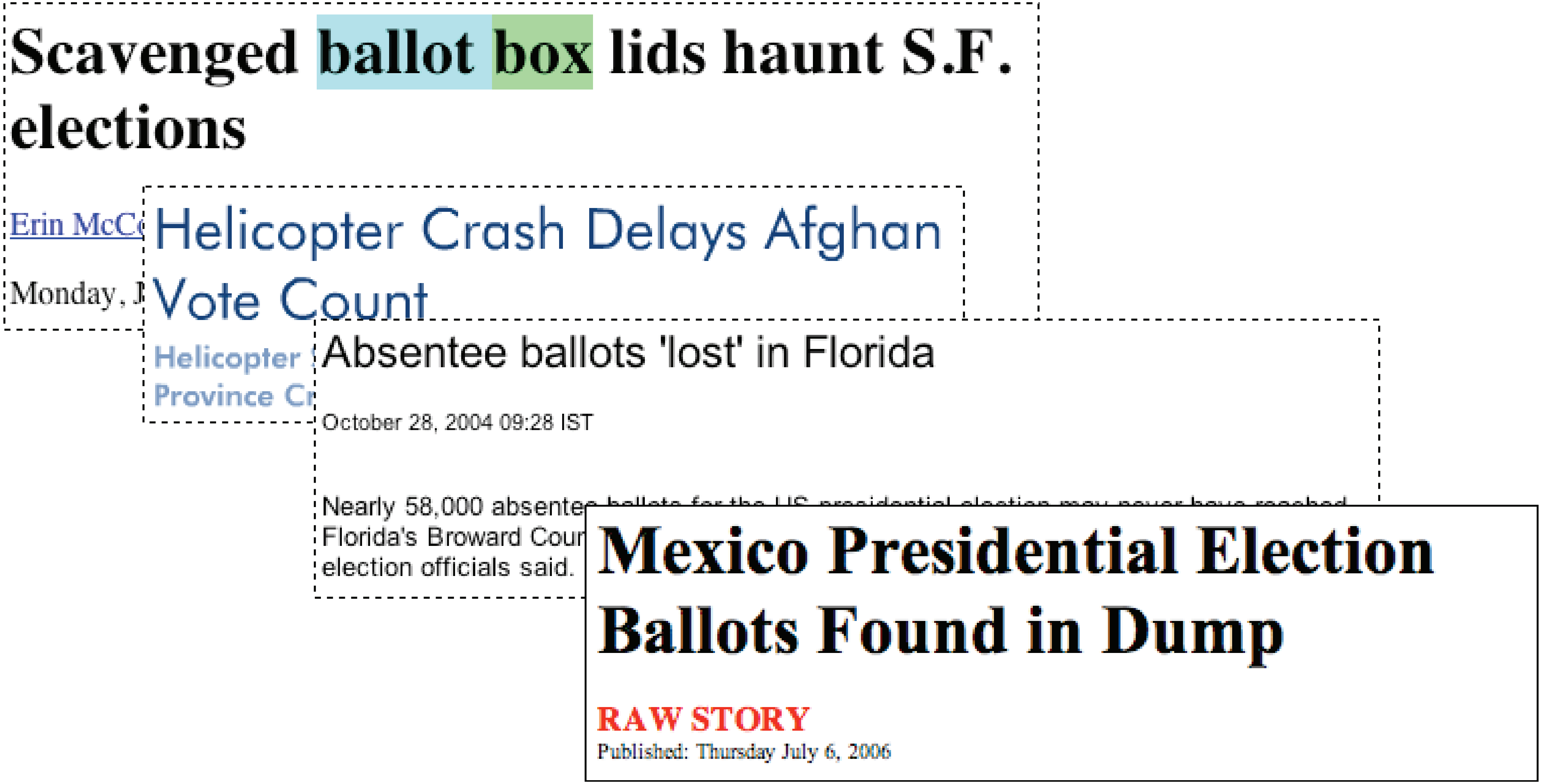
Province Cr

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward County voters, who had requested them more than two weeks ago, election officials said.

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, I

Helicopter Crash Delays Afghan Vote Count

Helicopter

Province Cr

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

Nearly 58,000 absente
Florida's Broward Cour
election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY
Published: Thursday July 6, 2006

Is Secrecy Important?

Is Secrecy Important?

> “Secret ballots and transparency in government are mutually exclusive concepts.”
>
> *Lynn Landes - Nov. 2005*

Is Secrecy Important?

> "Secret ballots and transparency in government are mutually exclusive concepts."
>
> *Lynn Landes - Nov. 2005*

USA

VOTE BY MAIL

THE VOTE BY MAIL PROJECT

http://votebymailproject.org

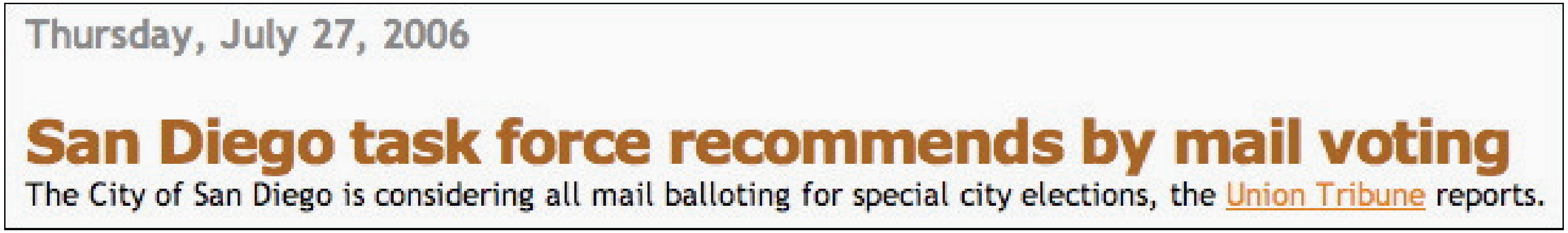
Is Secrecy Important?

"Secret ballots and transparency in government are mutually exclusive concepts."

Lynn Landes - Nov. 2005

THE VOTE BY MAIL PROJECT

http://votebymailproject.org



Thursday, July 27, 2006

San Diego task force recommends by mail voting

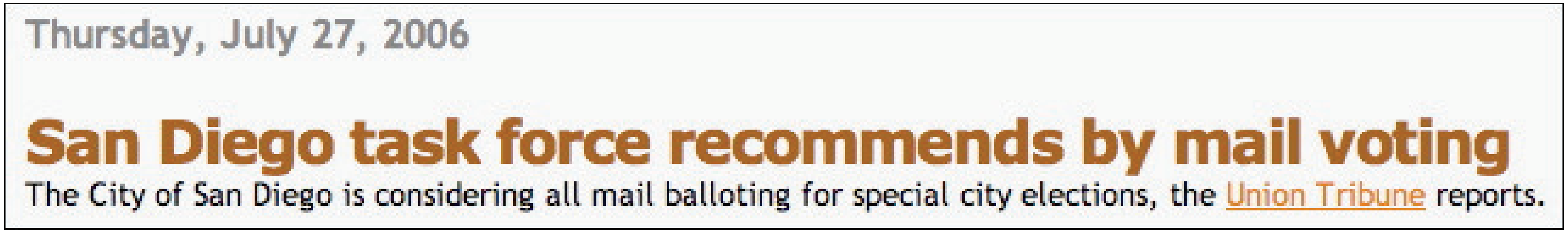
The City of San Diego is considering all mail balloting for special city elections, the Union Tribune reports.

Is Secrecy Important?

> “Secret ballots and transparency in government are mutually exclusive concepts.”
>
> *Lynn Landes - Nov. 2005*

THE VOTE BY MAIL PROJECT

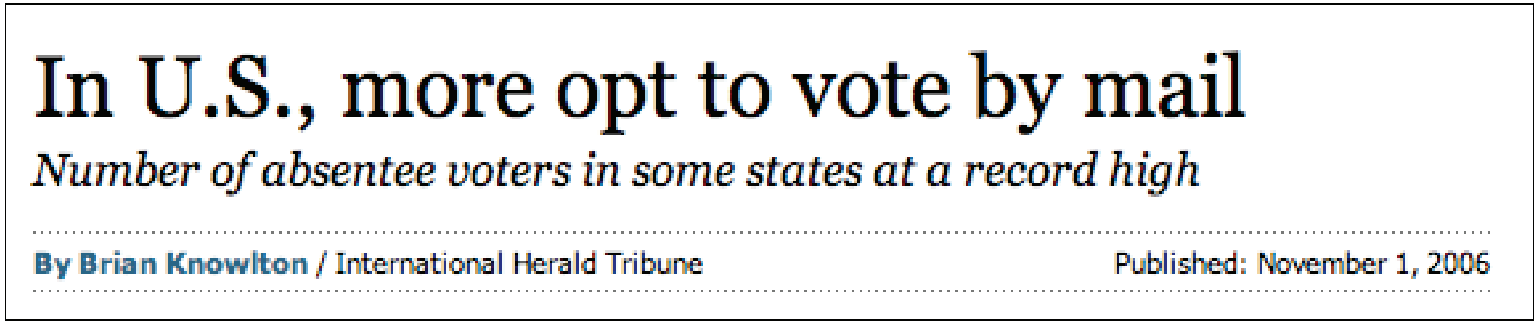
http://votebymailproject.org



Thursday, July 27, 2006

San Diego task force recommends by mail voting

The City of San Diego is considering all mail balloting for special city elections, the Union Tribune reports.



In U.S., more opt to vote by mail

Number of absentee voters in some states at a record high

By Brian Knowlton / International Herald Tribune

Published: November 1, 2006

Actually, it is.

Secret Ballot implemented in Chile in 1958.

“the **secrecy of the ballot** [...] has **first-order implications** for resource allocation, political outcomes, and social efficiency.”

[BalandRobinson 2004]

So what can we do?

Cryptographic (open audit) elections

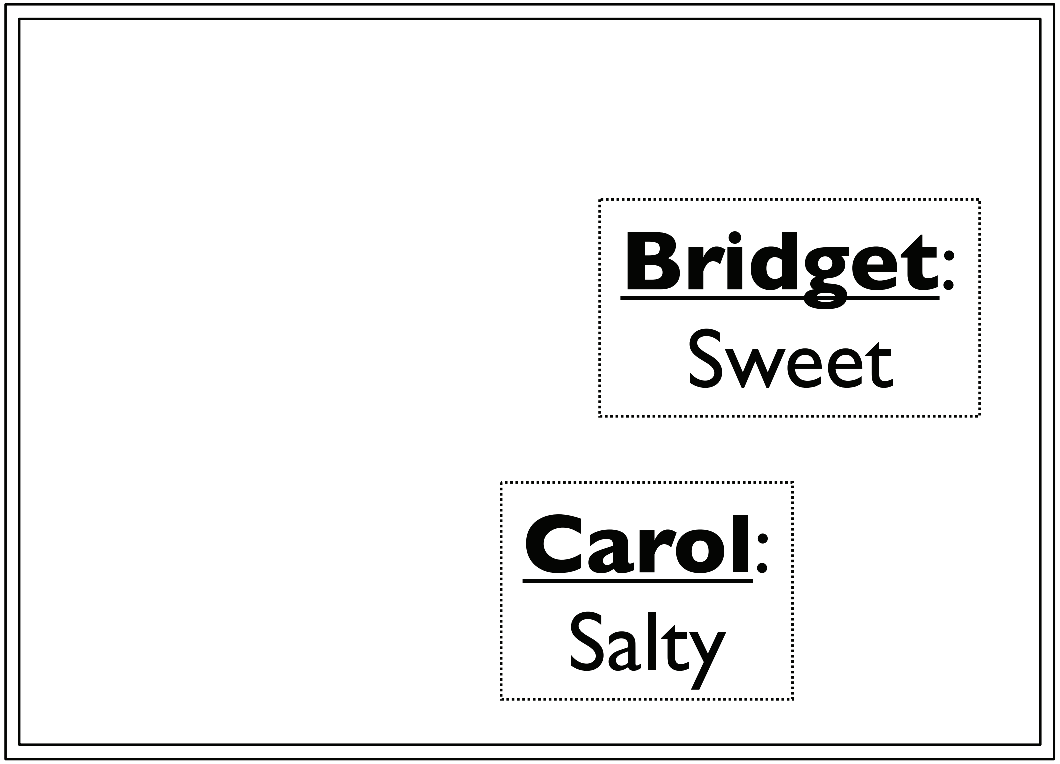
[Chaum81], [Benaloh85], [PIK93], [BenalohTuinstra92], [SK94], [Neff2001] , [FS2001], [Chaum2004], [Neff2004], [Ryan2004], [Chaum2005], [MoranNaor06], [Rivest2006],[CCCEPRRSS20080]

Cryptography provides more than confidentiality.

Cryptography can provide **verifiability** while mantaining **ballot secrecy**.

Anyone can audit!

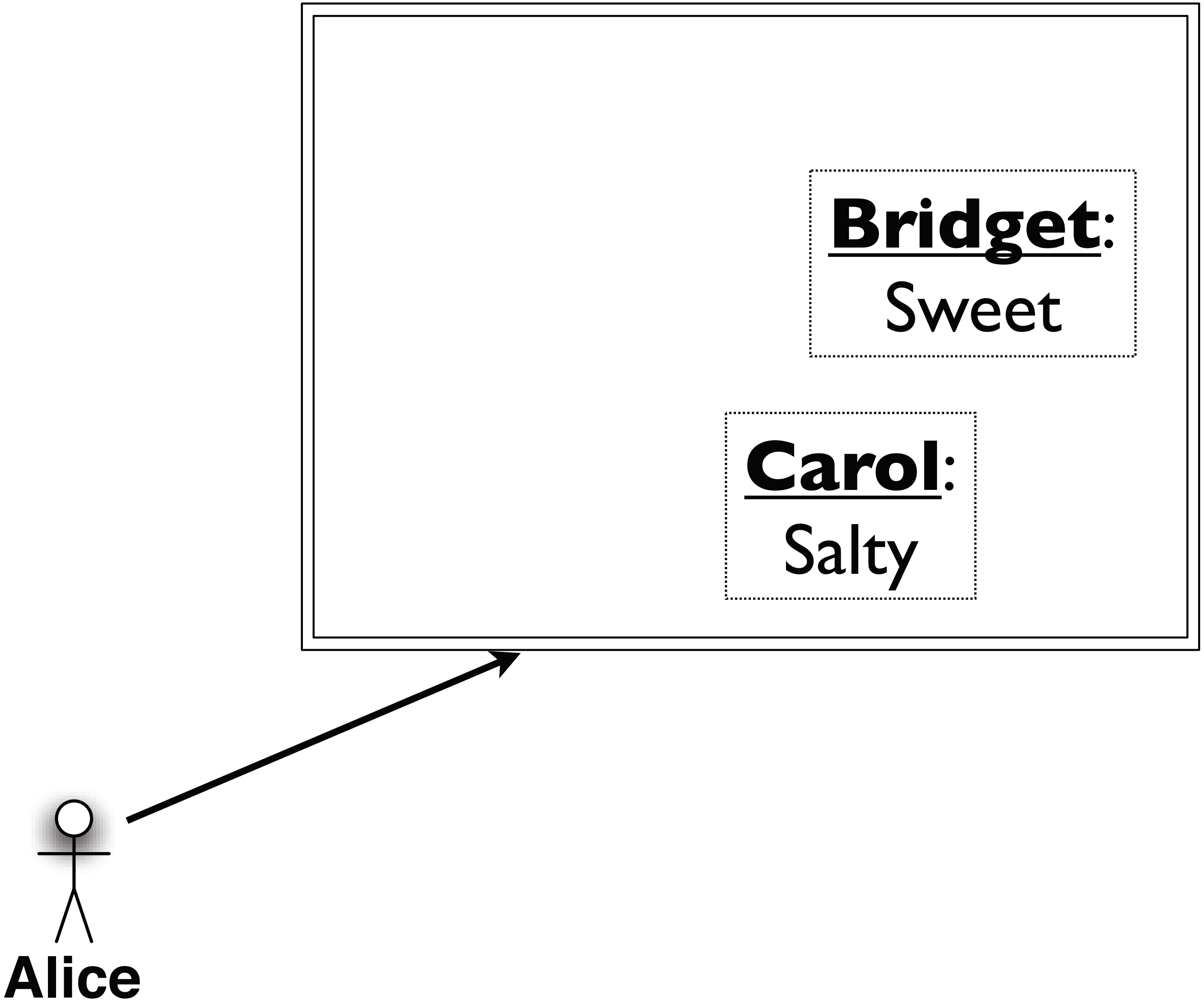
Public Ballots



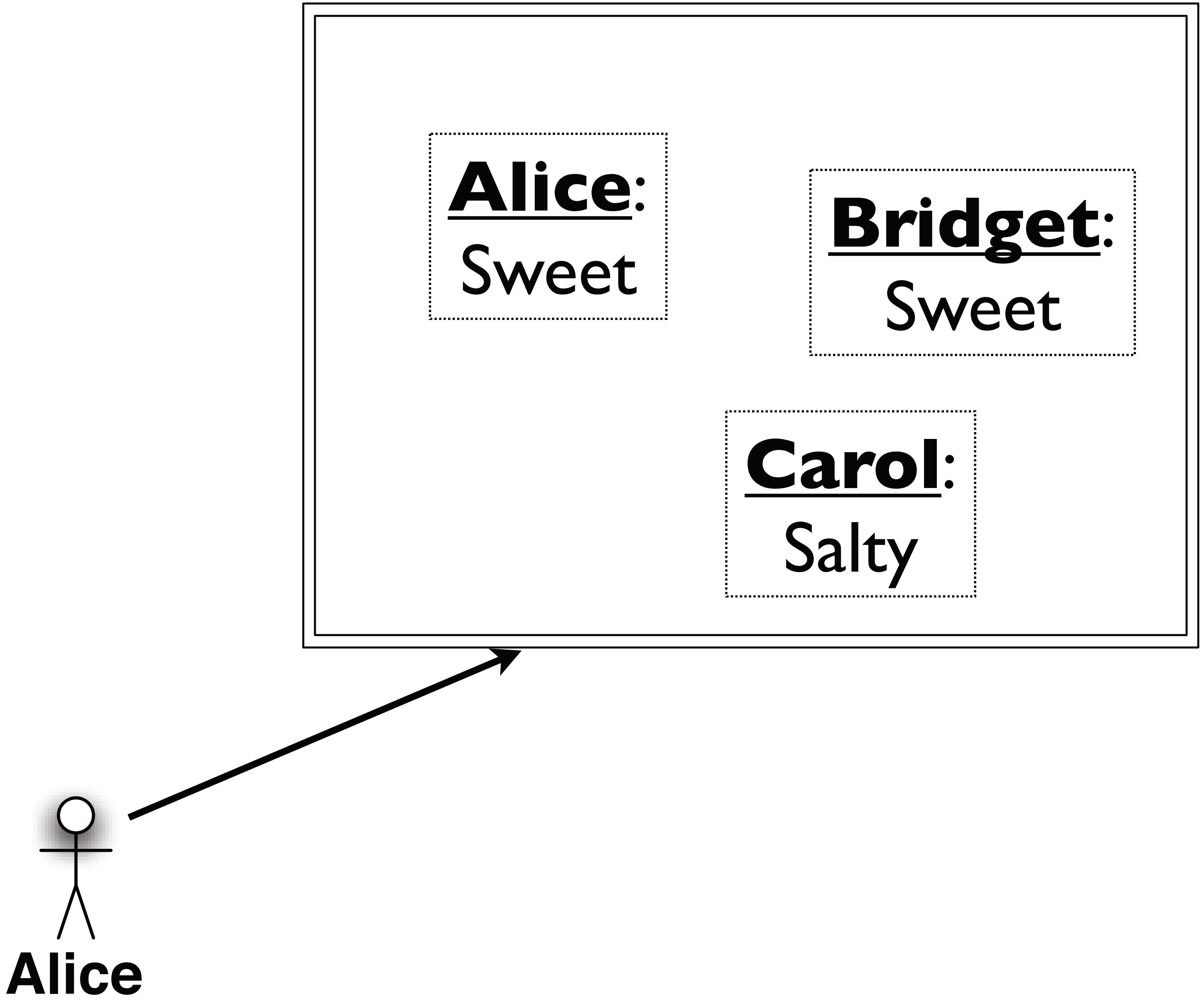
Bridget:
Sweet

Carol:
Salty

Public Ballots



Public Ballots



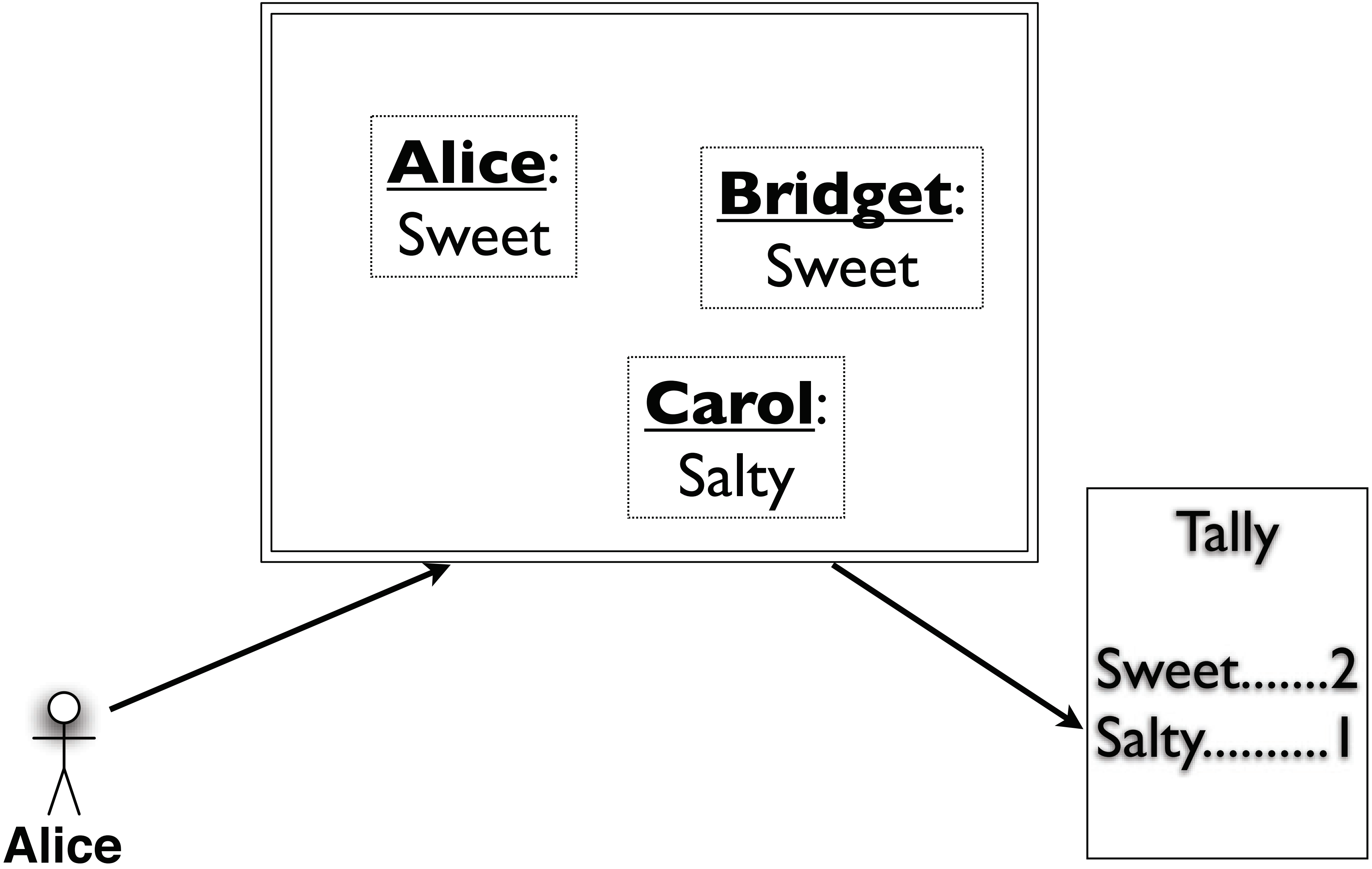
Alice: Sweet

Bridget: Sweet

Carol: Salty

Alice

Public Ballots



Alice: Sweet

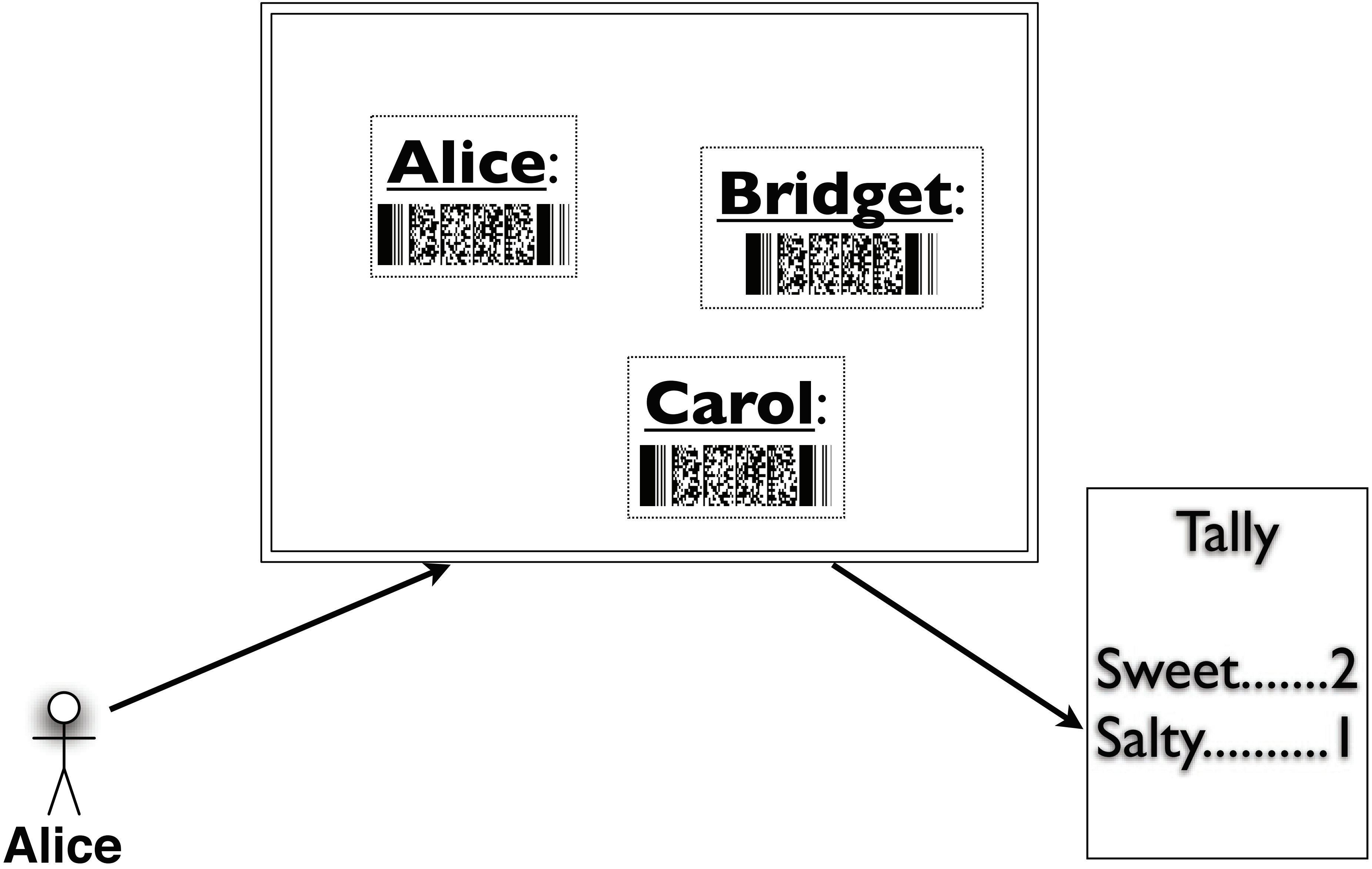
Bridget: Sweet

Carol: Salty

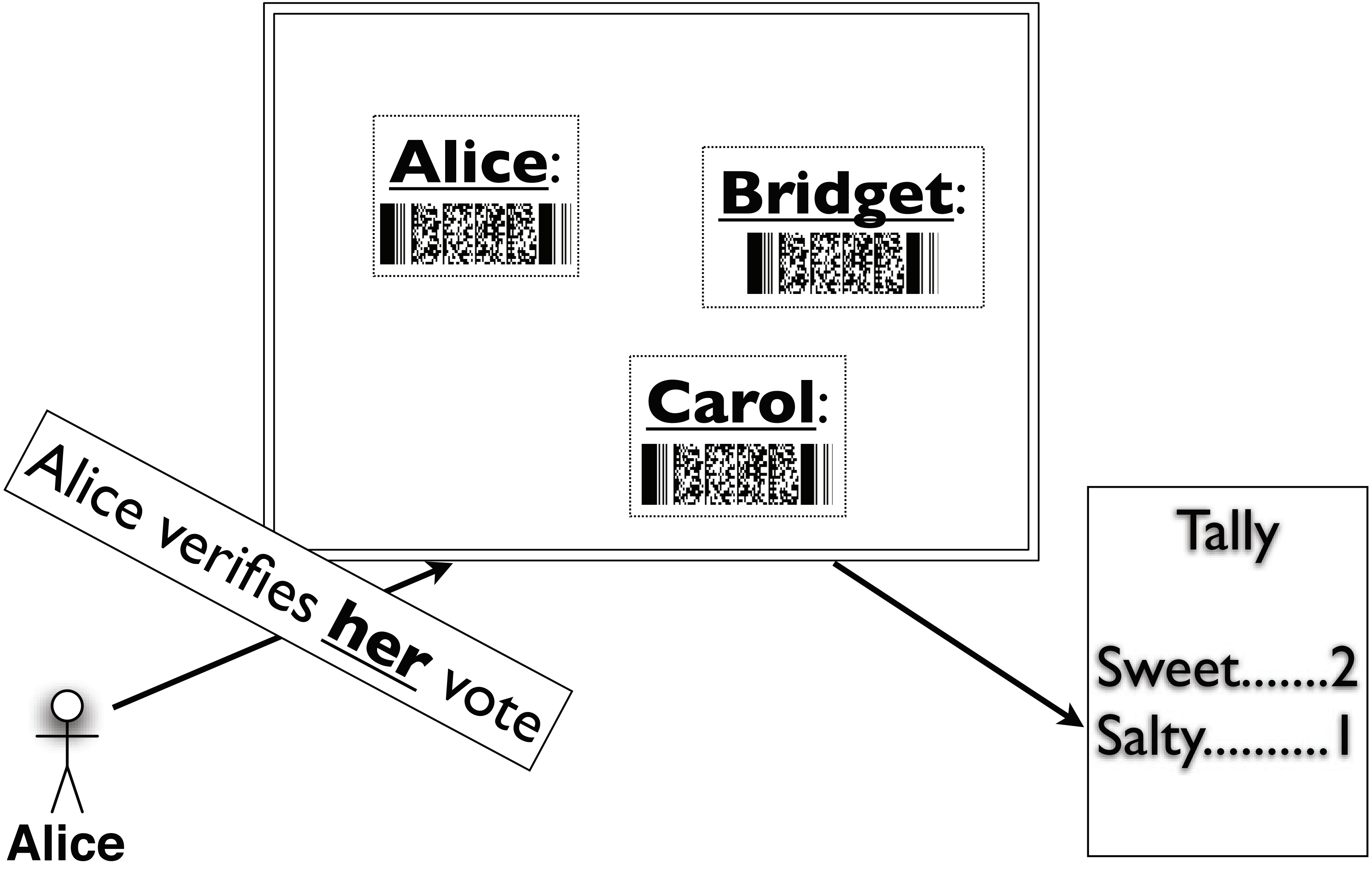
Tally

Sweet.......2
Salty.........1

Encrypted Public Ballots



Encrypted Public Ballots



Alice:

Bridget:

Carol:

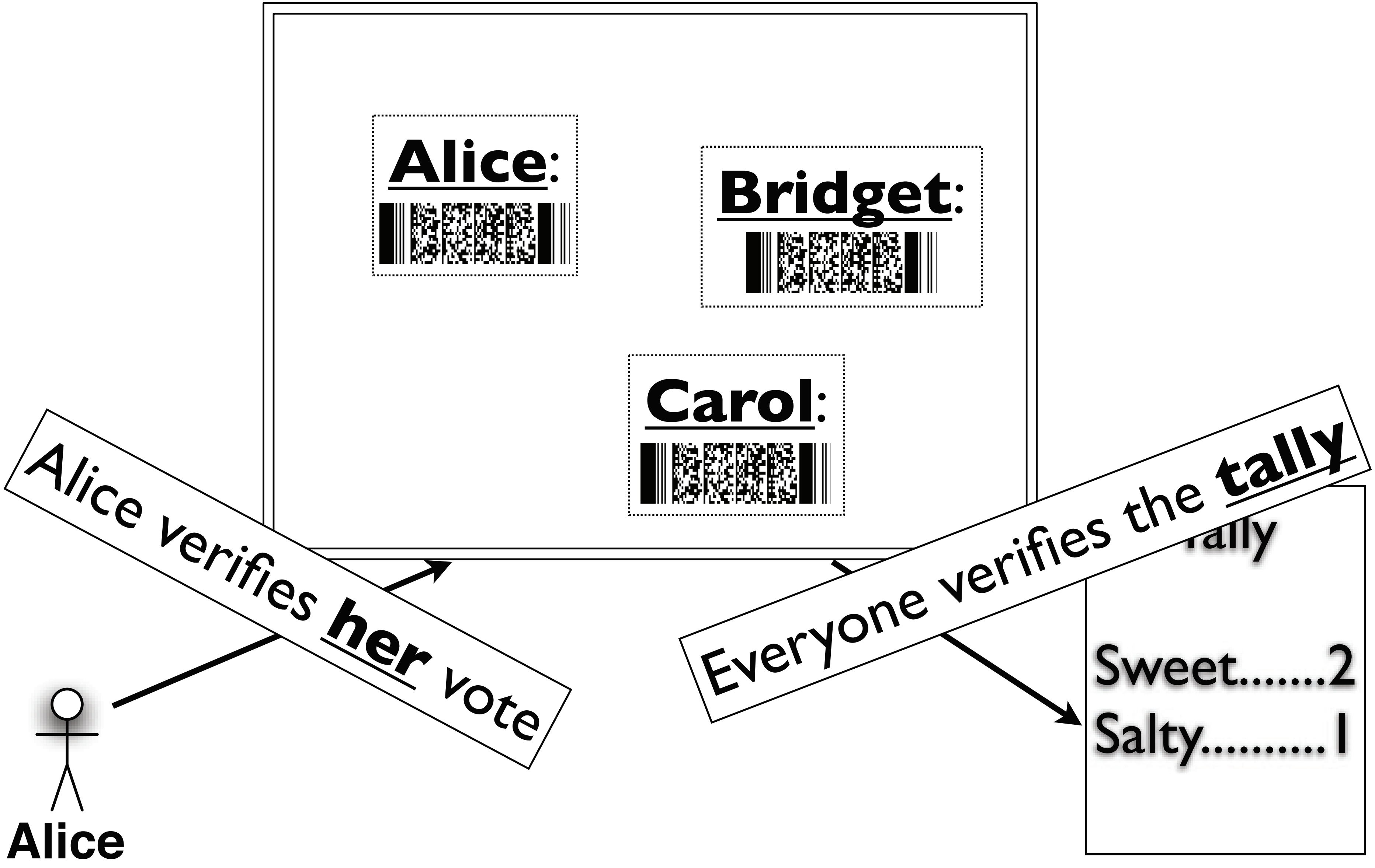
Alice verifies **her** vote

Alice

Tally

Sweet.......2
Salty.........1

Encrypted Public Ballots



Alice:

Bridget:

Carol:

Tally

Sweet.......2
Salty.........1

Alice

Alice verifies **her** vote

Everyone verifies the **tally**

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

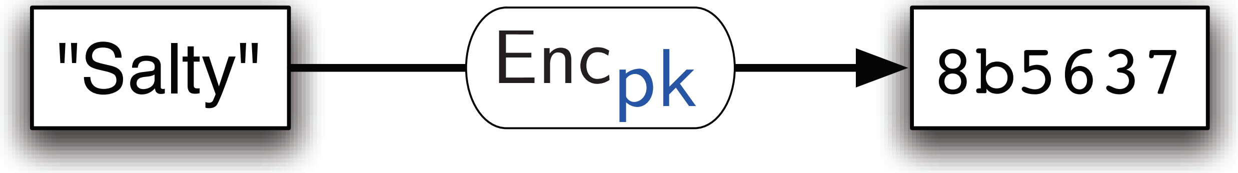
Public-Key Encryption

Public-Key Encryption

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

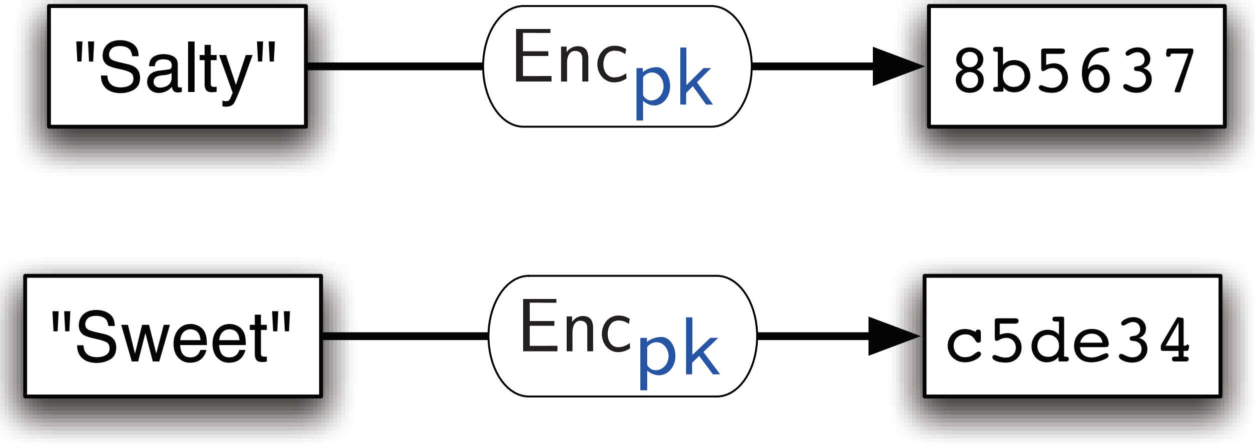
Public-Key Encryption

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



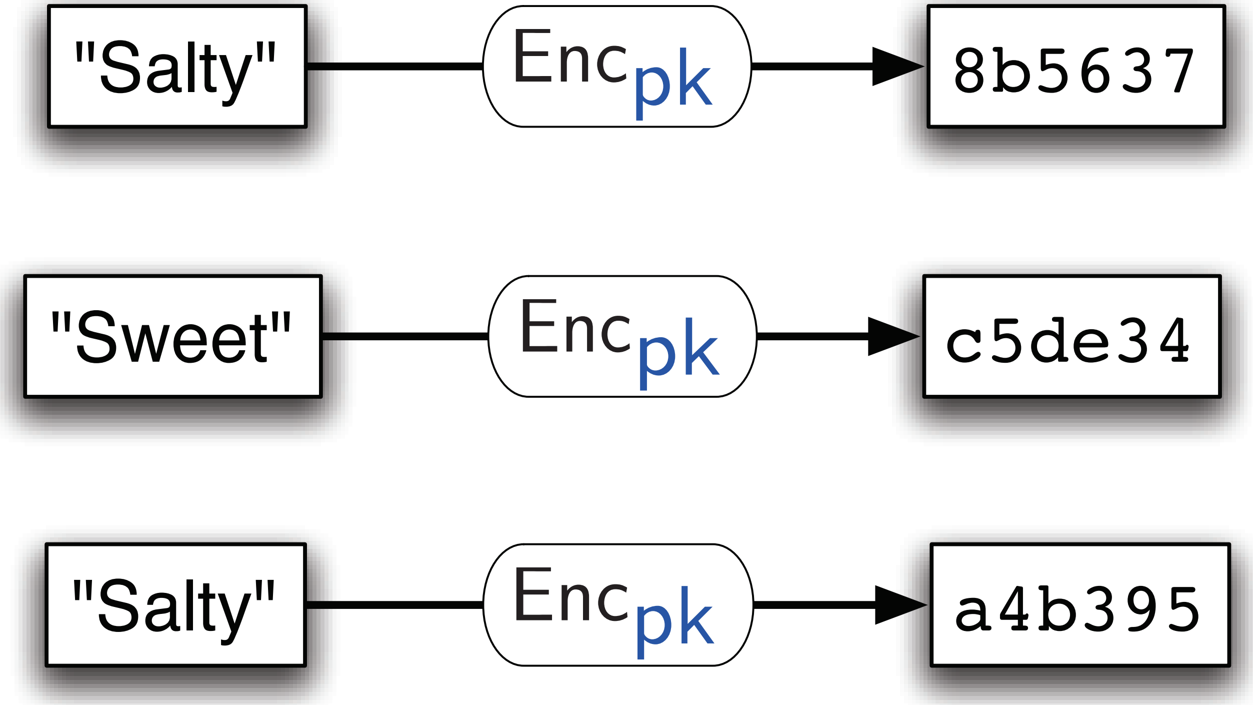
Public-Key Encryption

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.



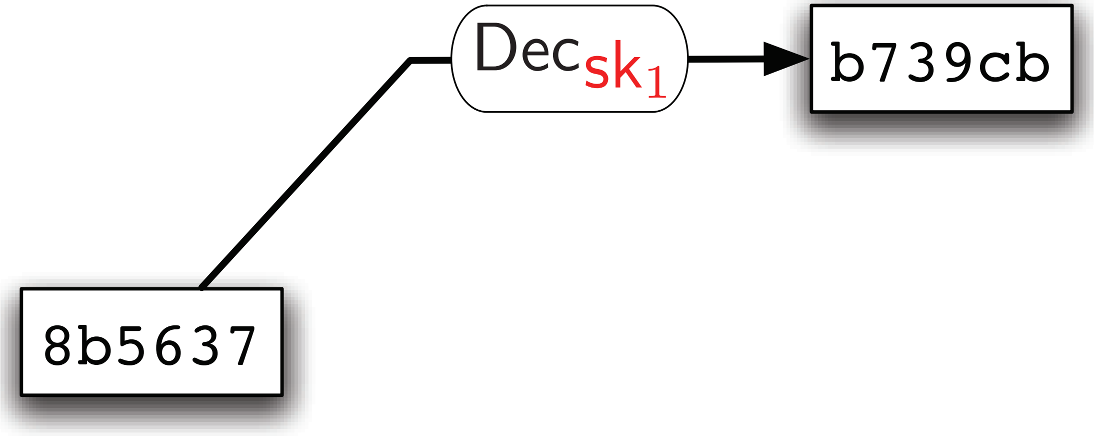
Threshold Decryption

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

8b5637

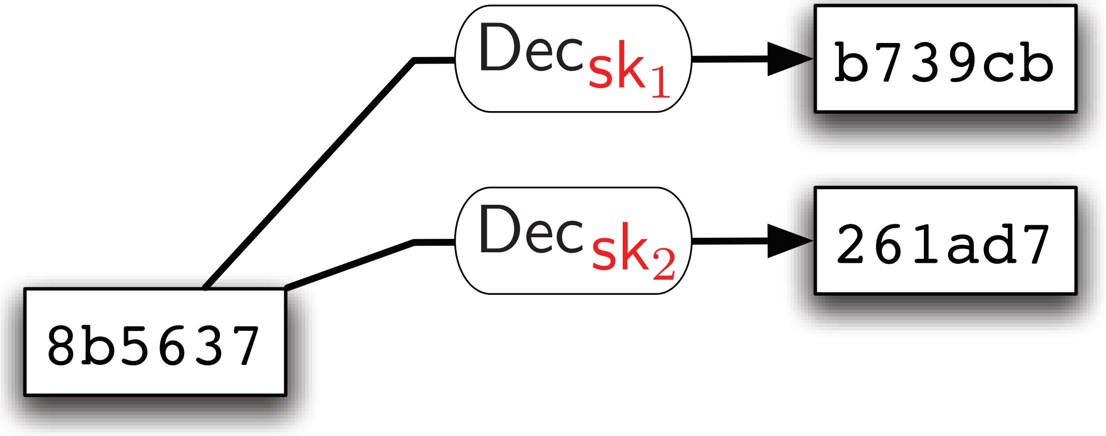
Threshold Decryption

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



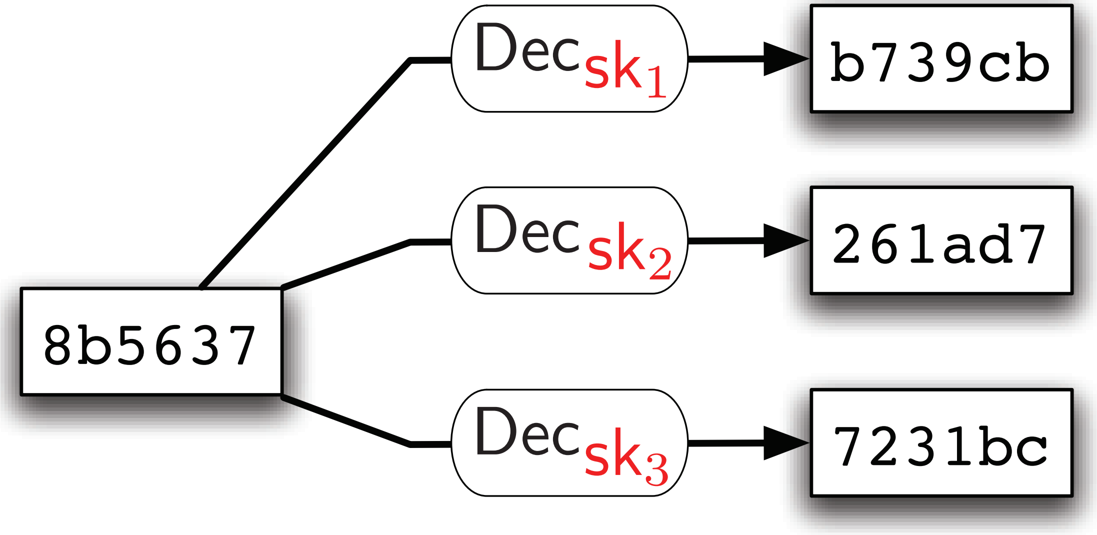
Threshold Decryption

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



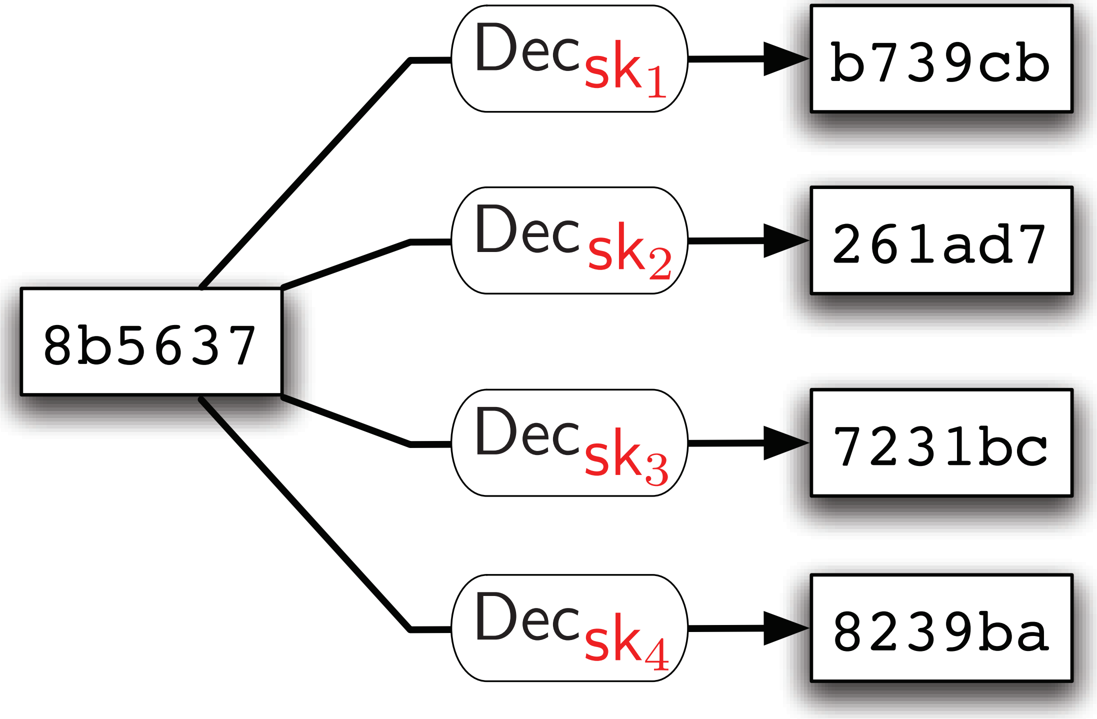
Threshold Decryption

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



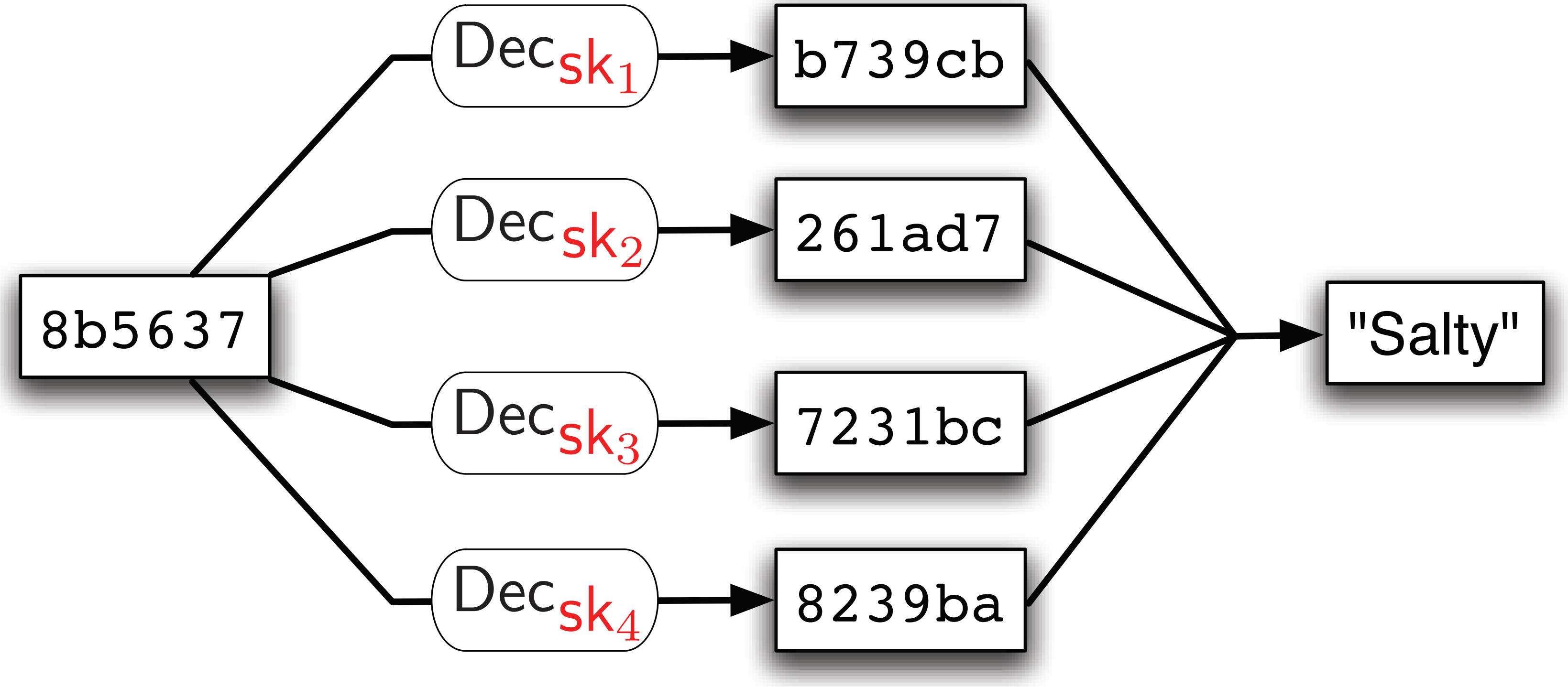
Threshold Decryption

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



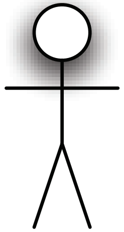
Threshold Decryption

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

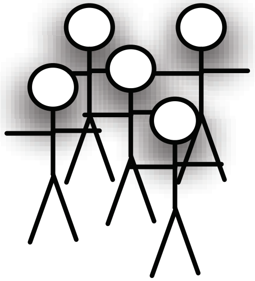

8b5637
$\mathrm{Dec}_{\mathrm{sk}_1}$
$\mathrm{Dec}_{\mathrm{sk}_2}$
$\mathrm{Dec}_{\mathrm{sk}_3}$
$\mathrm{Dec}_{\mathrm{sk}_4}$
b739cb
261ad7
7231bc
8239ba
"Salty"

The Voting Process

Identification

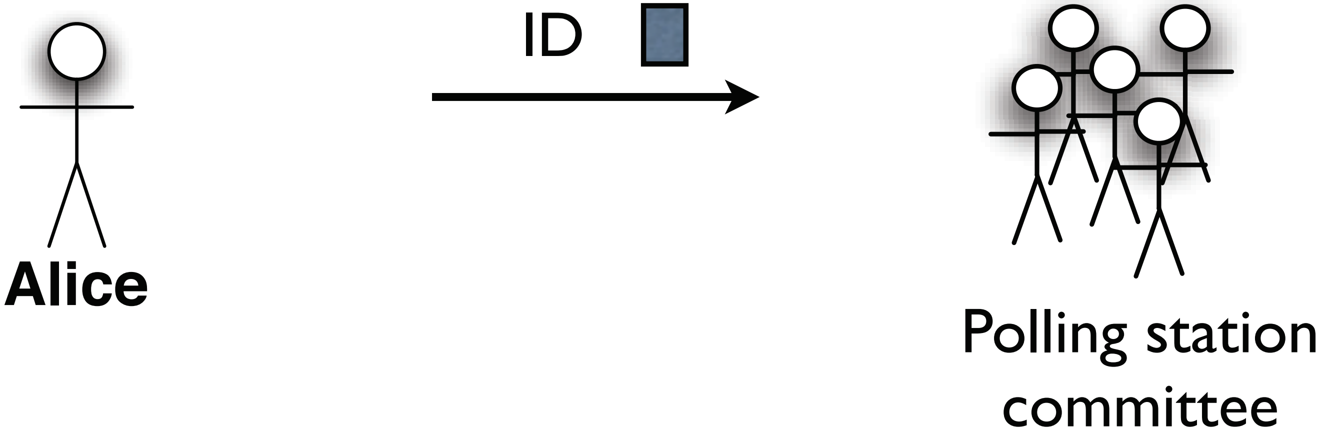


Alice

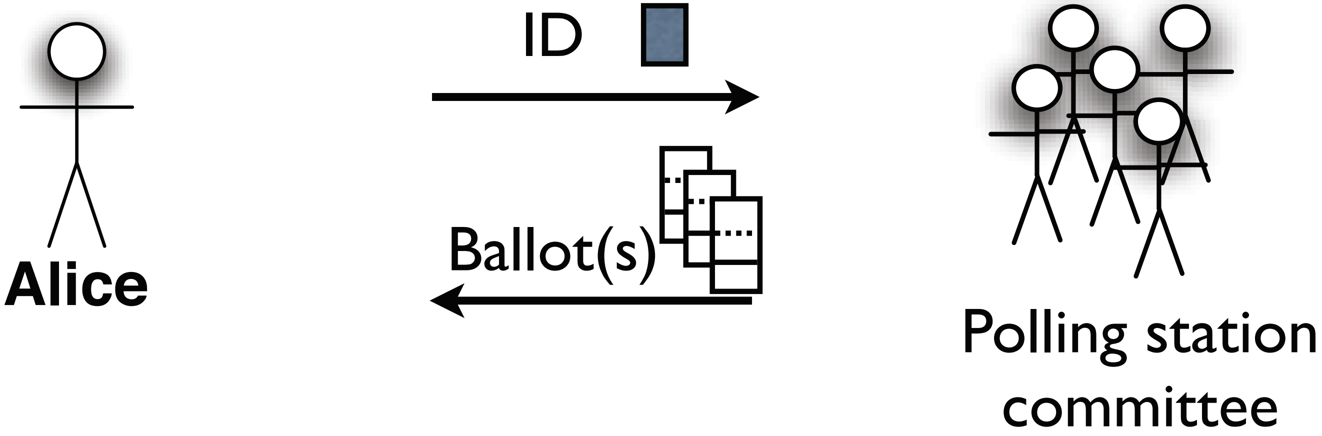


Polling station committee

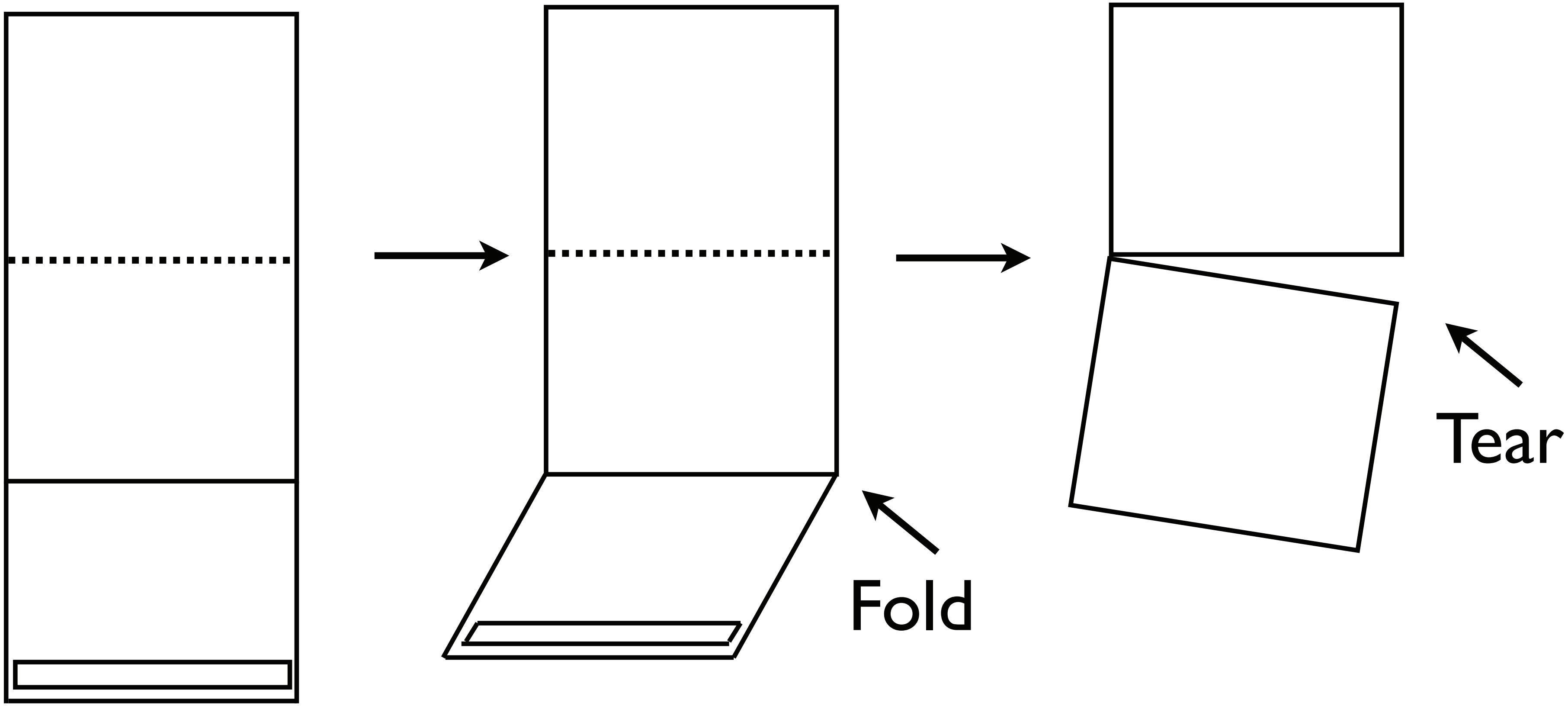
Identification



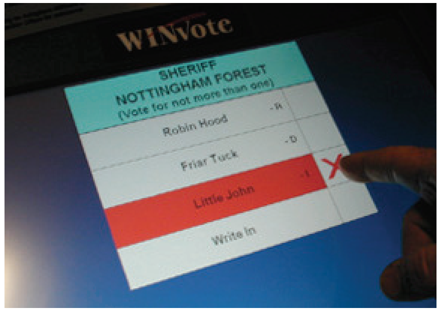
Identification



The Ballot



Producing Encrypted Ballot



WINVote

SHERIFF
NOTTINGHAM FOREST
(Vote for not more than one)

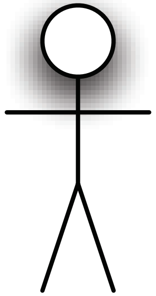
Robin Hood -R

Friar Tuck -D

Little John -I

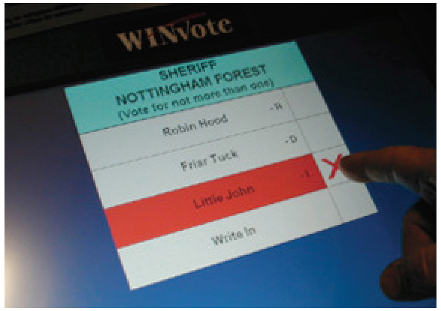
Write In

+



Alice

Producing Encrypted Ballot



WINVote

SHERIFF
NOTTINGHAM FOREST
(Vote for not more than one)

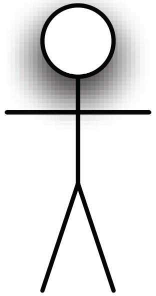
Robin Hood -R

Friar Tuck -D

Little John -I

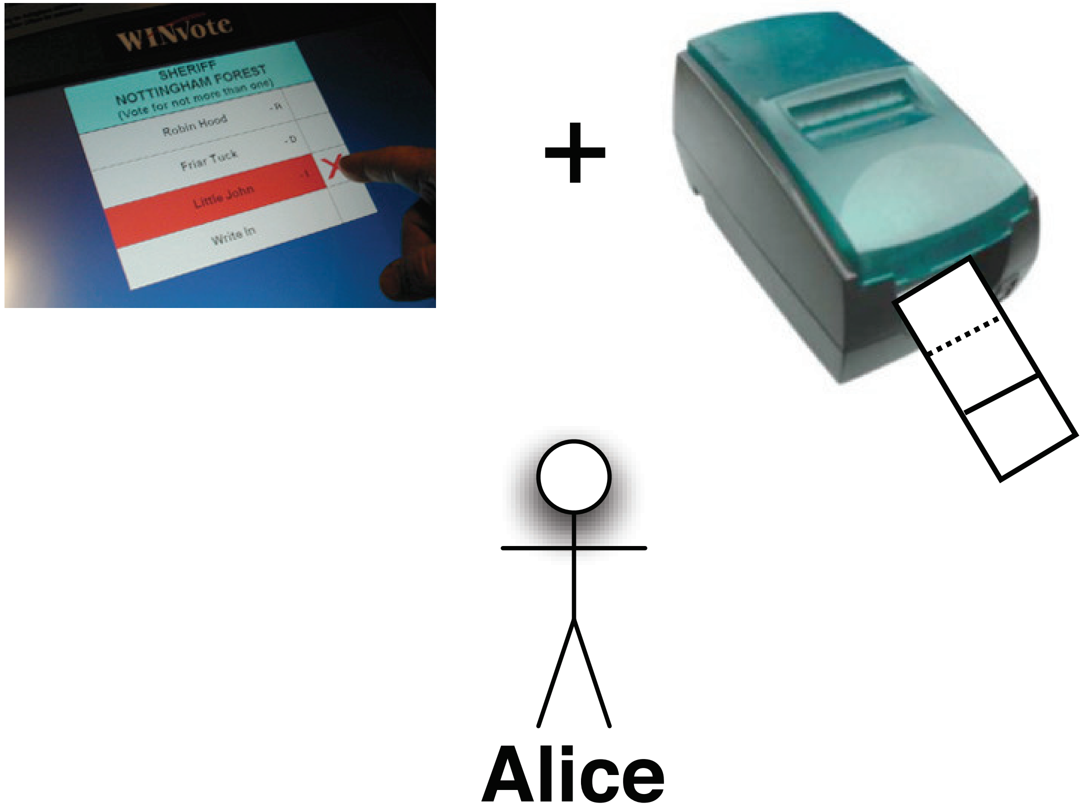
Write In

+

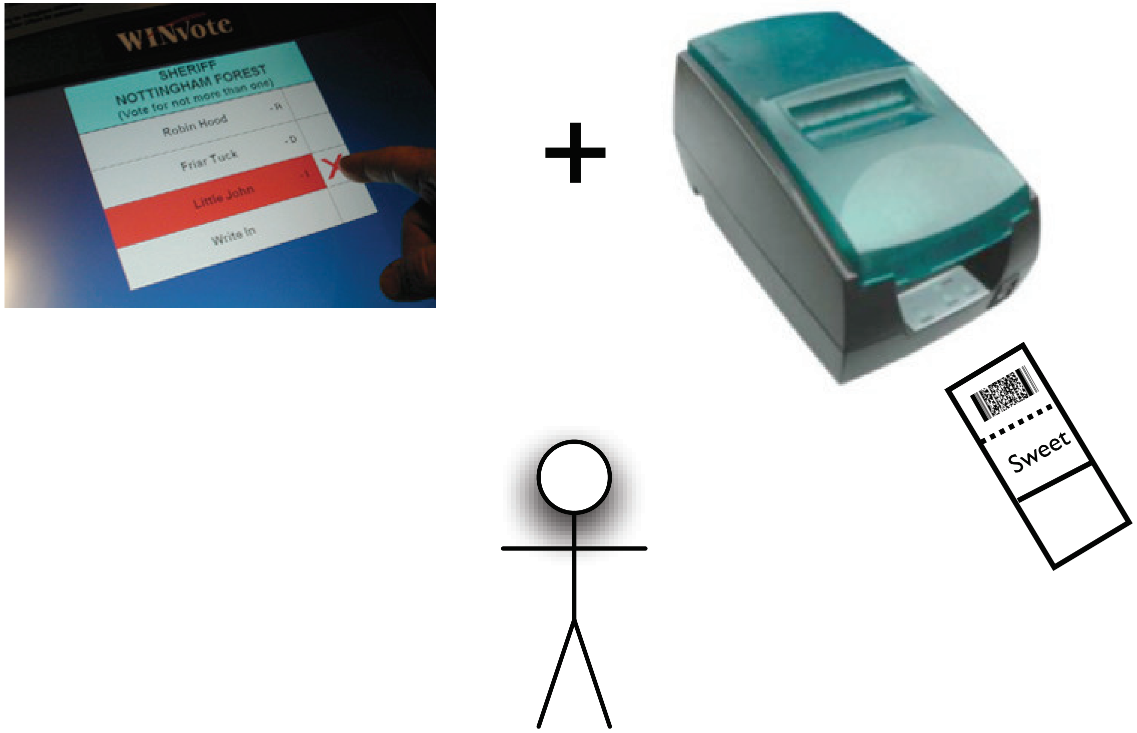


Alice

Producing Encrypted Ballot

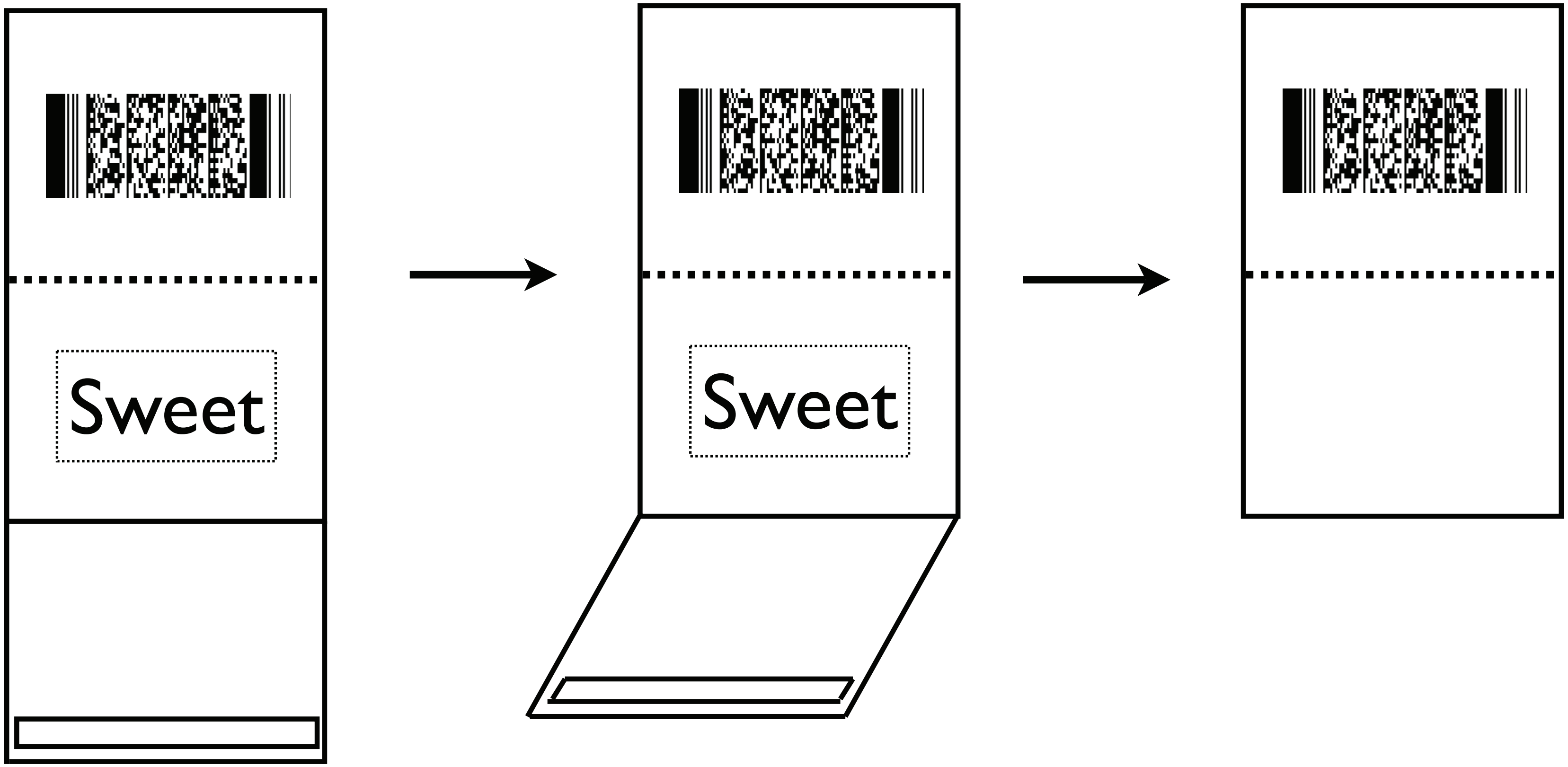


Producing Encrypted Ballot

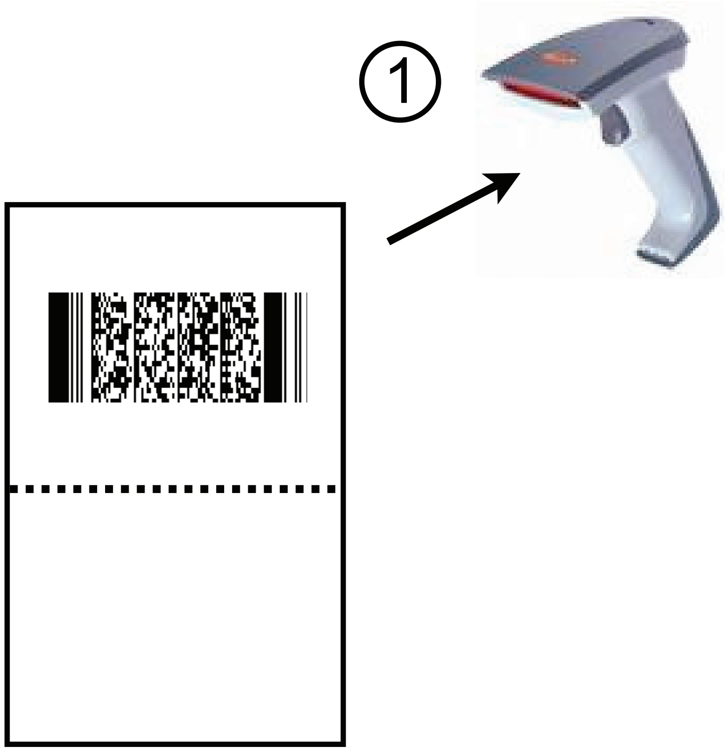


Alice

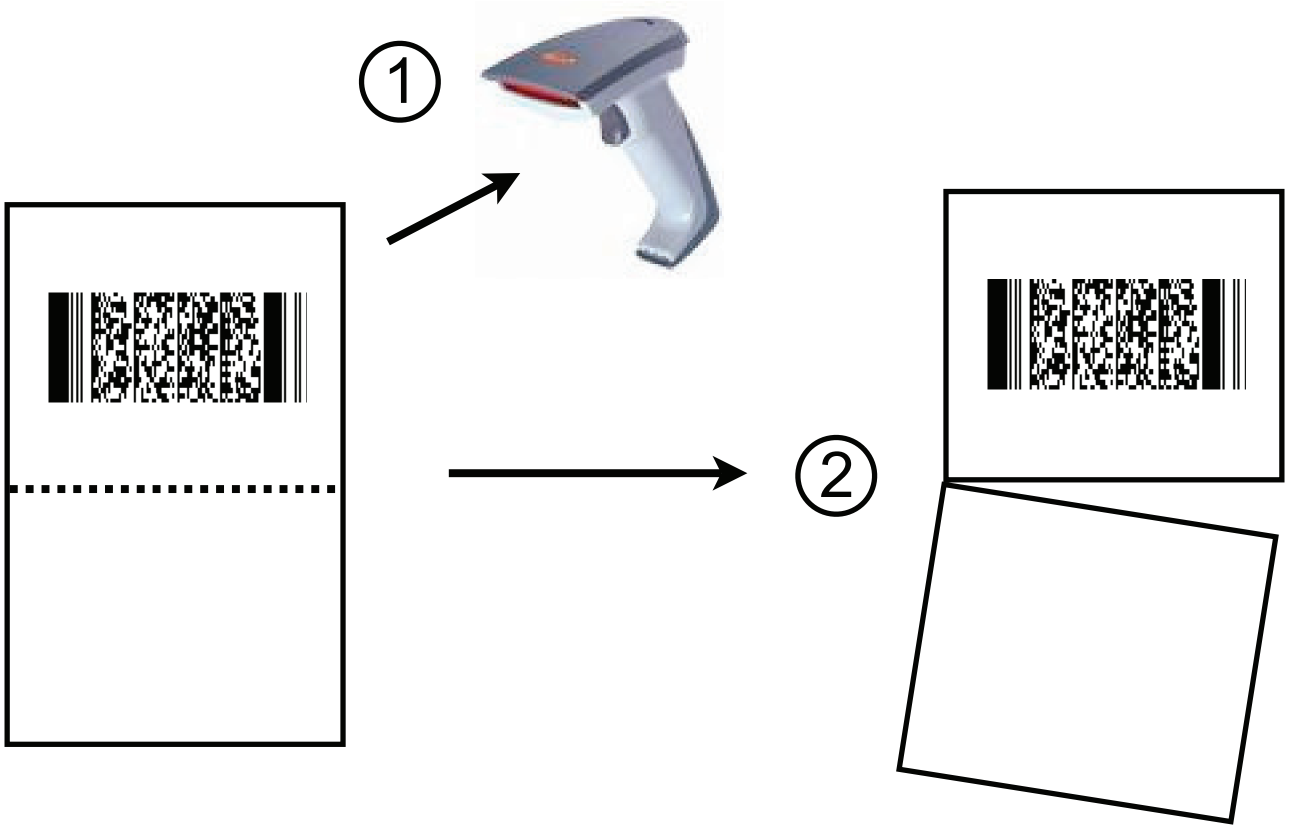
Encrypted Ballot



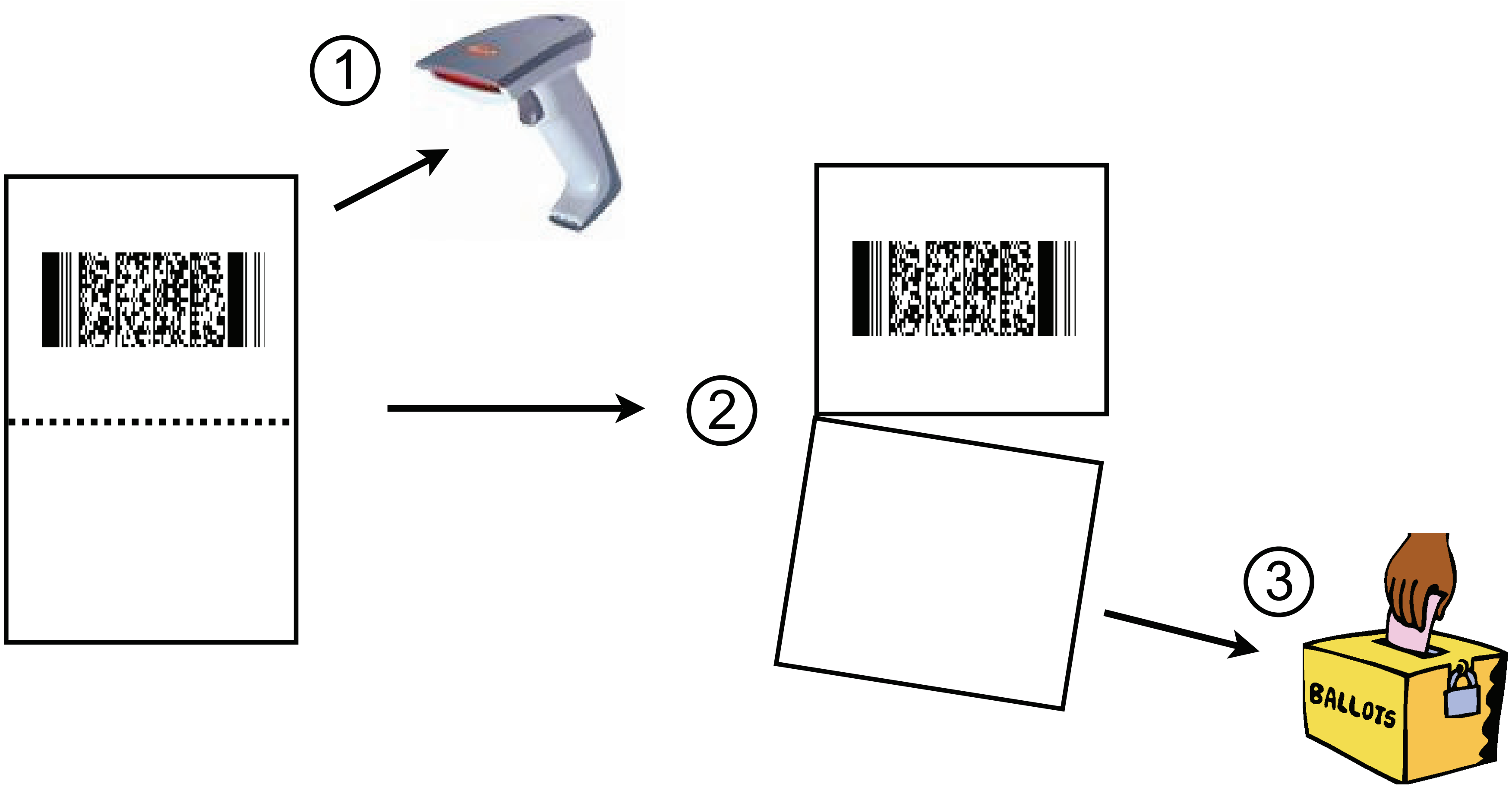
Ballot Casting



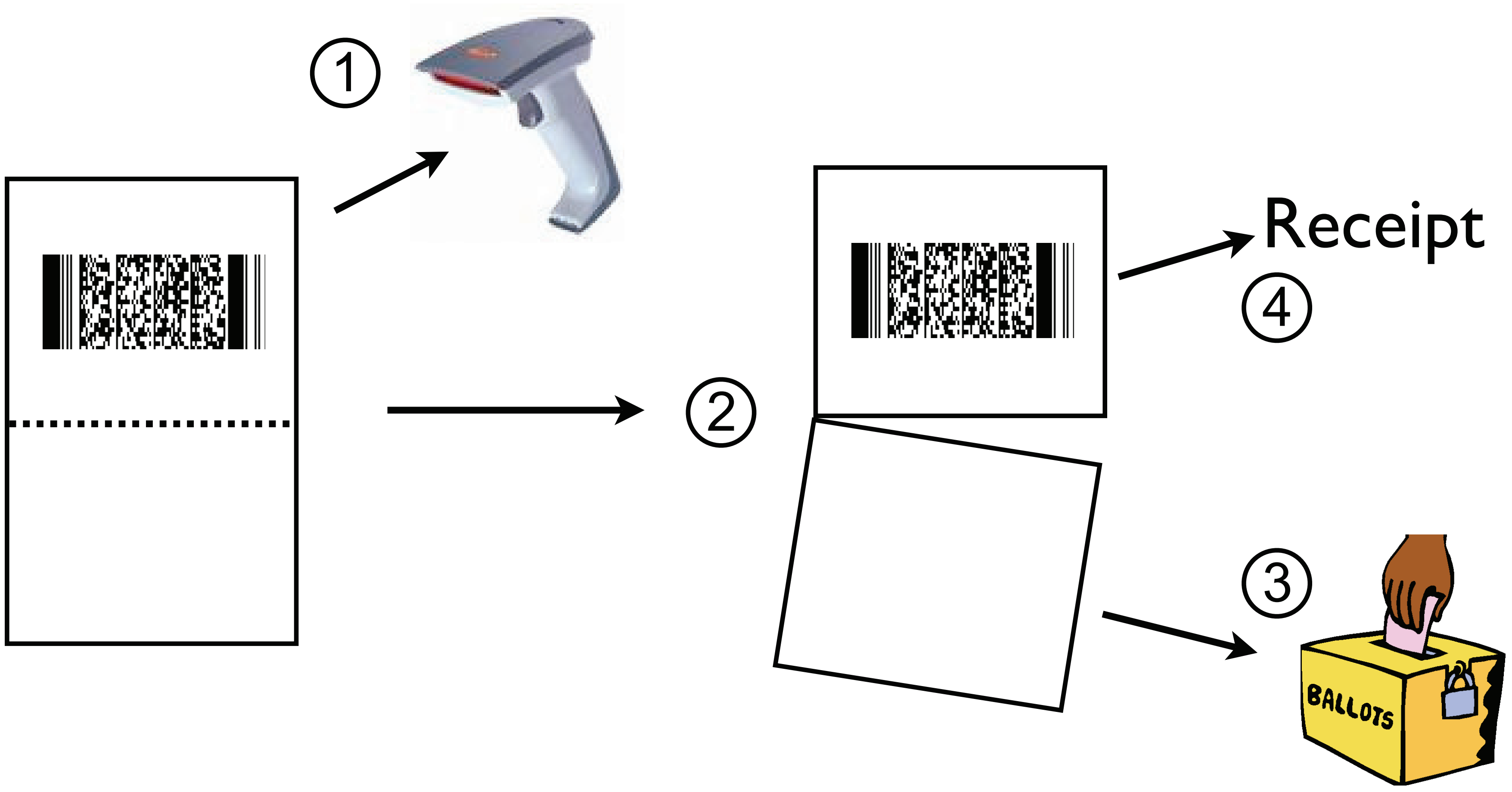
Ballot Casting



Ballot Casting



Ballot Casting



①

②

③

④

Receipt

Homomorphic Tabulation

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

Homomorphic Tabulation

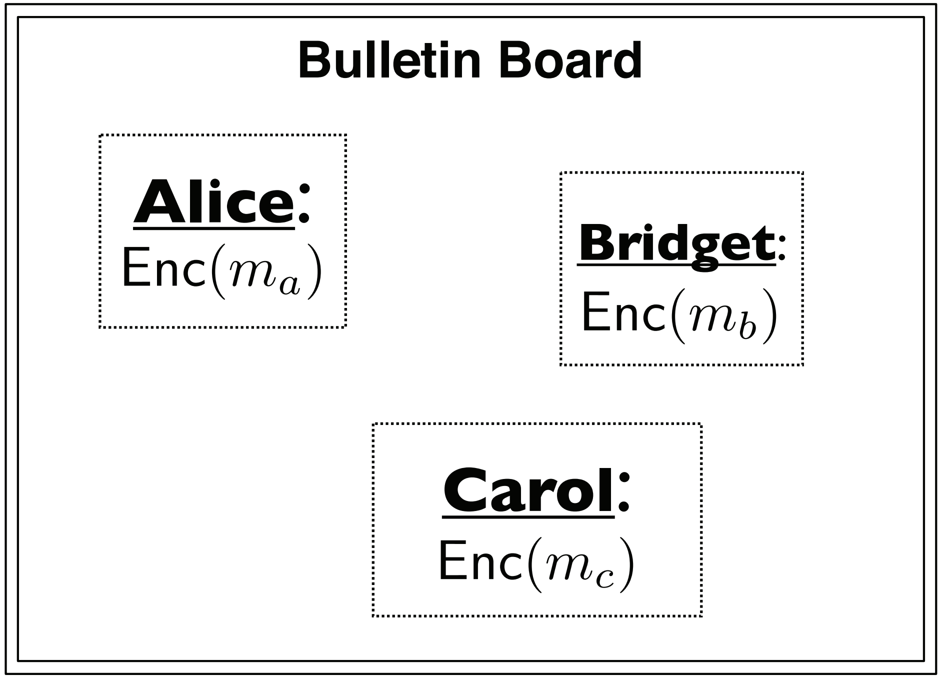
$$\mathsf{Enc}(m_1) \times \mathsf{Enc}(m_2)$$
$$= \mathsf{Enc}(m_1 + m_2)$$

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

Homomorphic Tabulation

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

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



Bulletin Board

Alice: $\text{Enc}(m_a)$

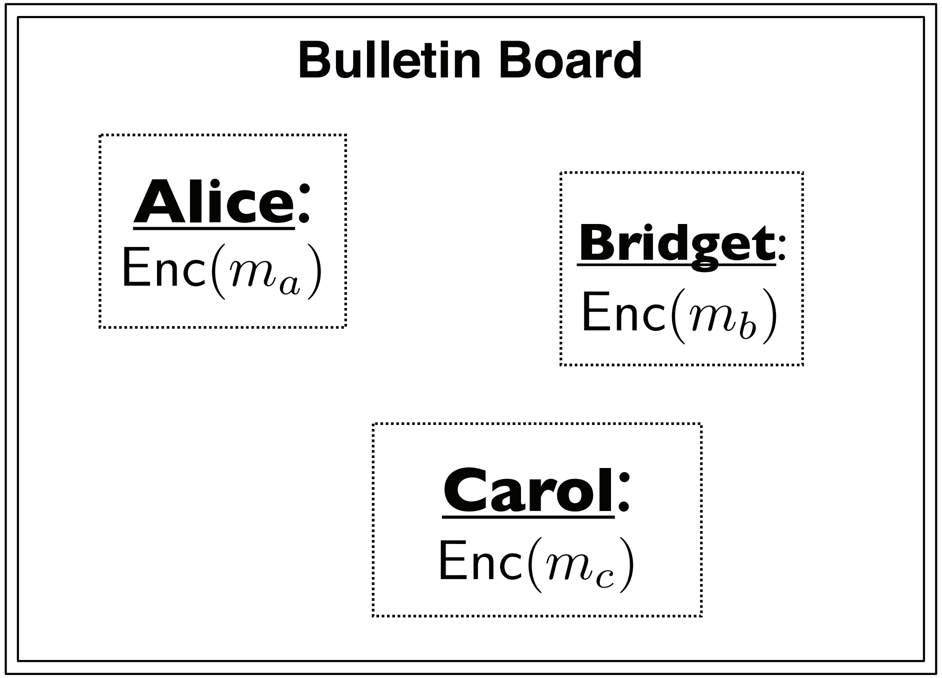
Bridget: $\text{Enc}(m_b)$

Carol: $\text{Enc}(m_c)$

Homomorphic Tabulation

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

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



Bulletin Board

Alice: Enc(m_a)

Bridget: Enc(m_b)

Carol: Enc(m_c)

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

Verifying Validity of Encryption

Given Enc(*m*) How can I verify that it is not an encryption of more than one vote?

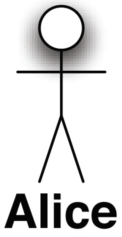
Zero-Knowledge proofs: Can prove validity of Enc(*m*) without revealing anything else!

Revolutionary concept: only need to verify that machine is computing right functionality...

Verifying Consistency [Benaloh]

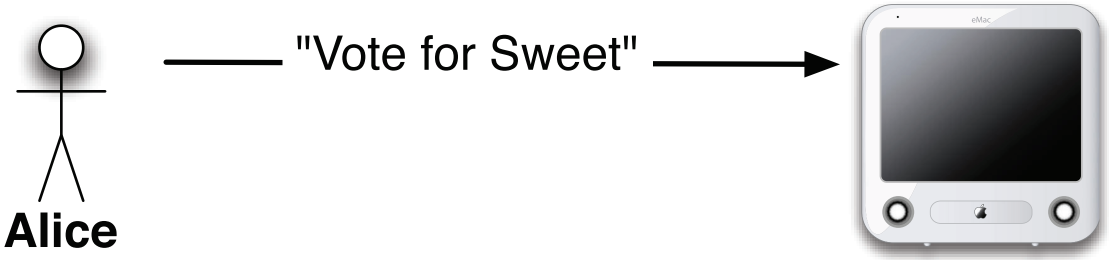
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



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

Verifying Consistency [Benaloh]

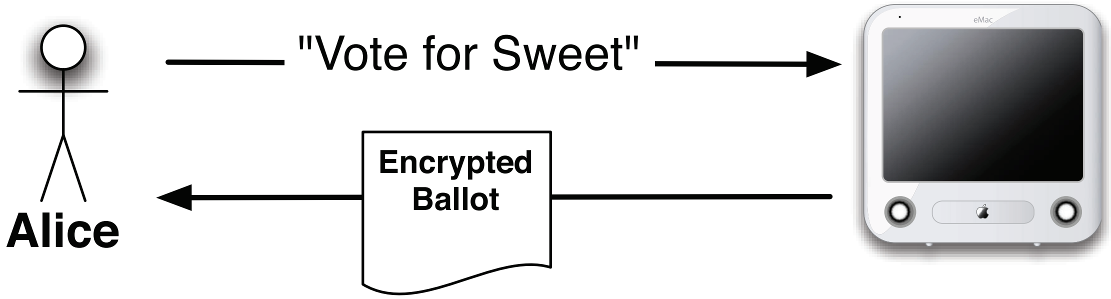


Alice

"Vote for Sweet"

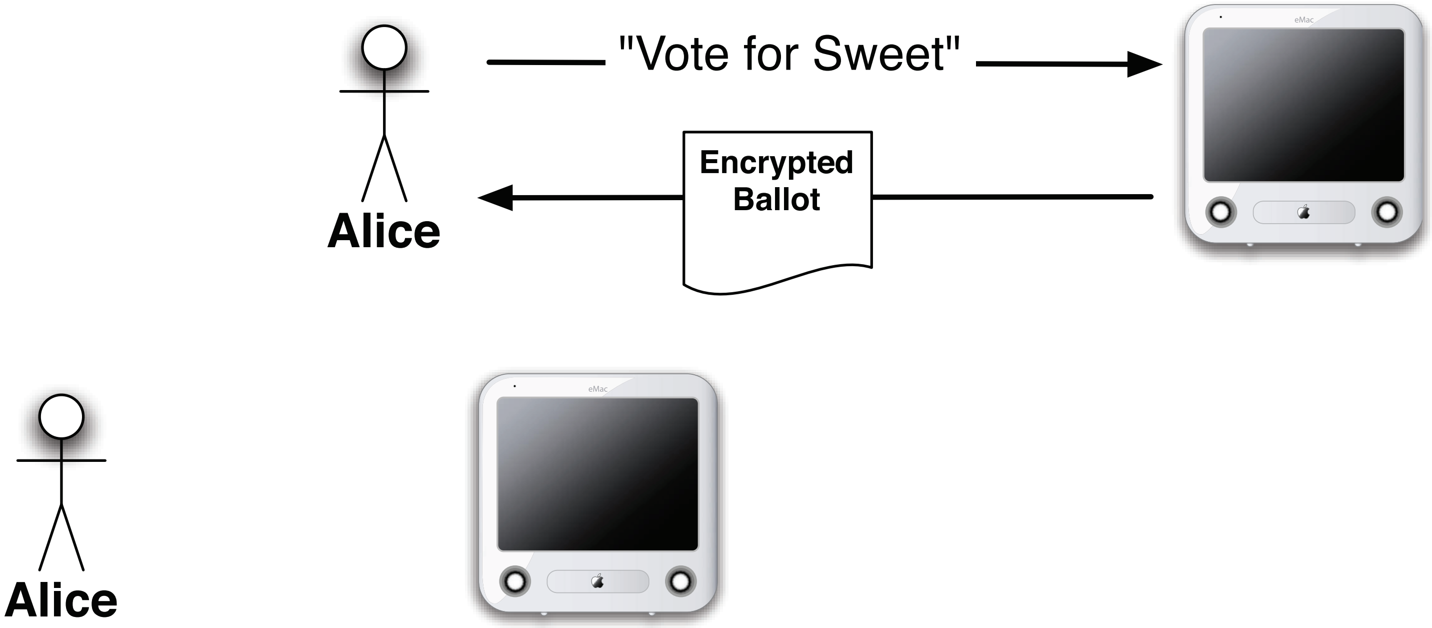
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



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

Verifying Consistency [Benaloh]



Alice

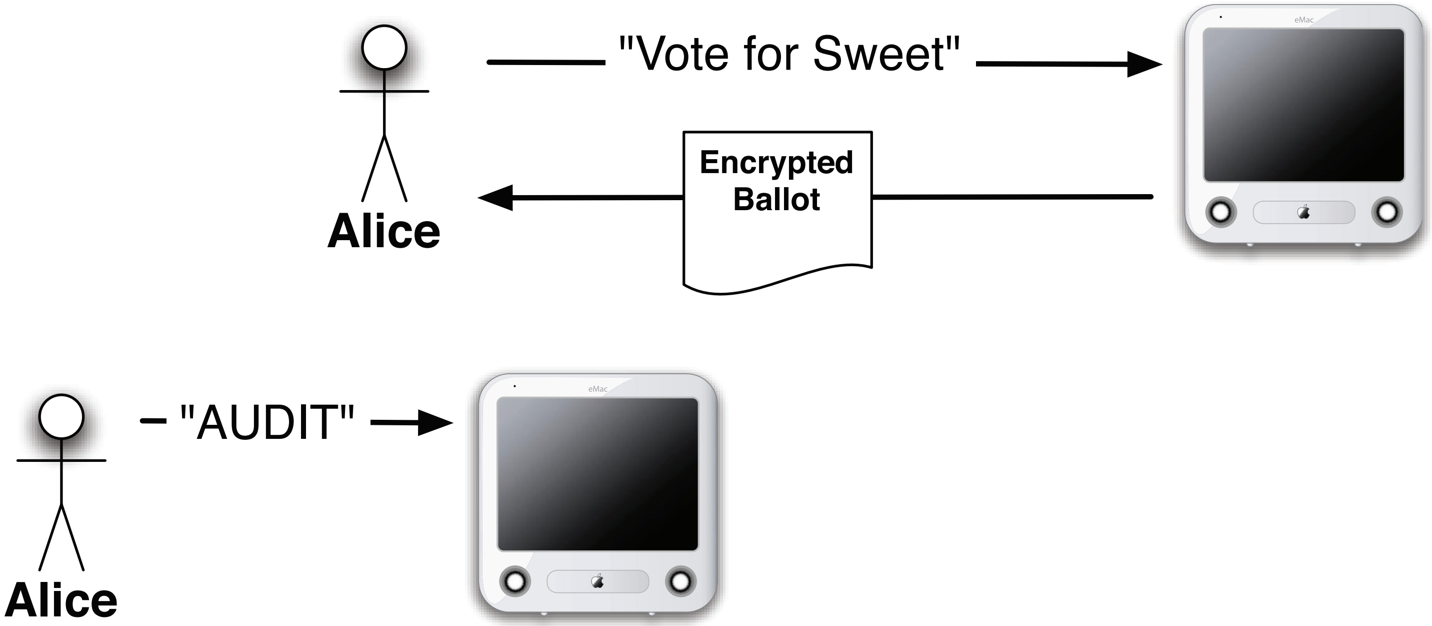
"Vote for Sweet"

Encrypted Ballot

Alice

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

Verifying Consistency [Benaloh]



"Vote for Sweet"

Encrypted Ballot

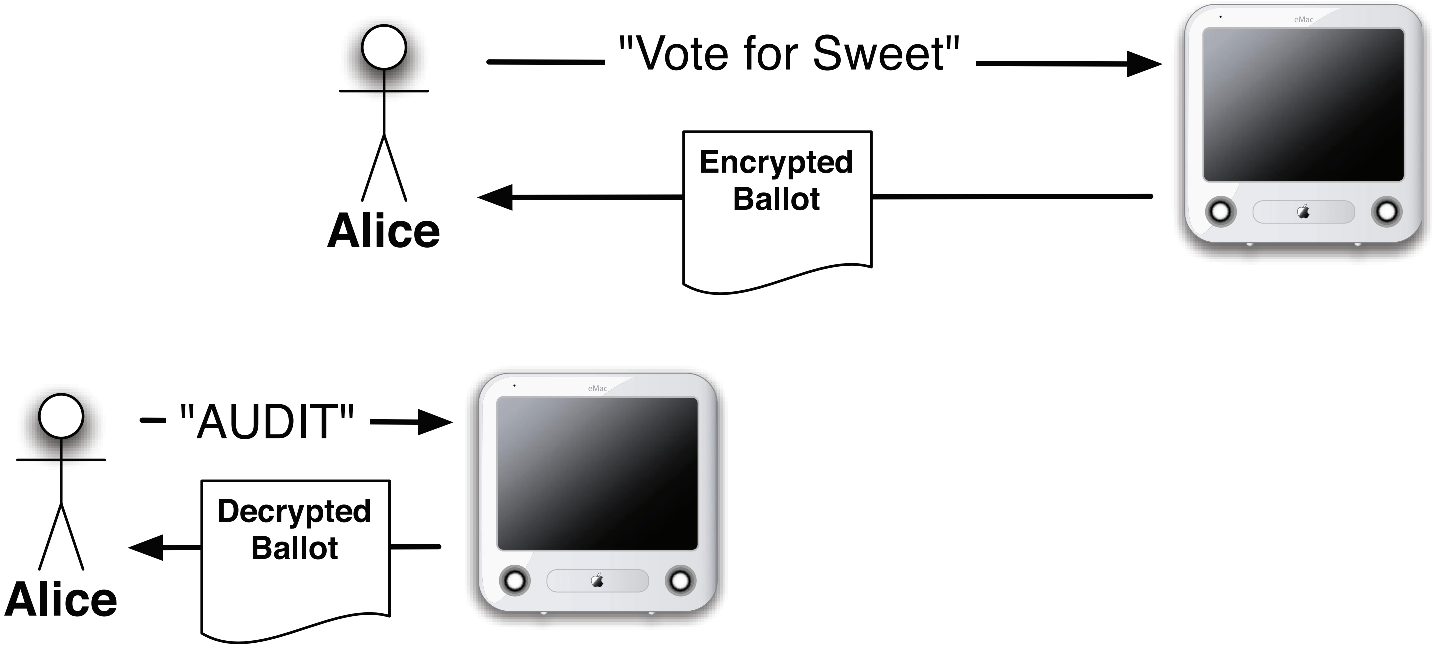
Alice

"AUDIT"

Alice

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

Verifying Consistency [Benaloh]



Alice

"Vote for Sweet"

Encrypted Ballot

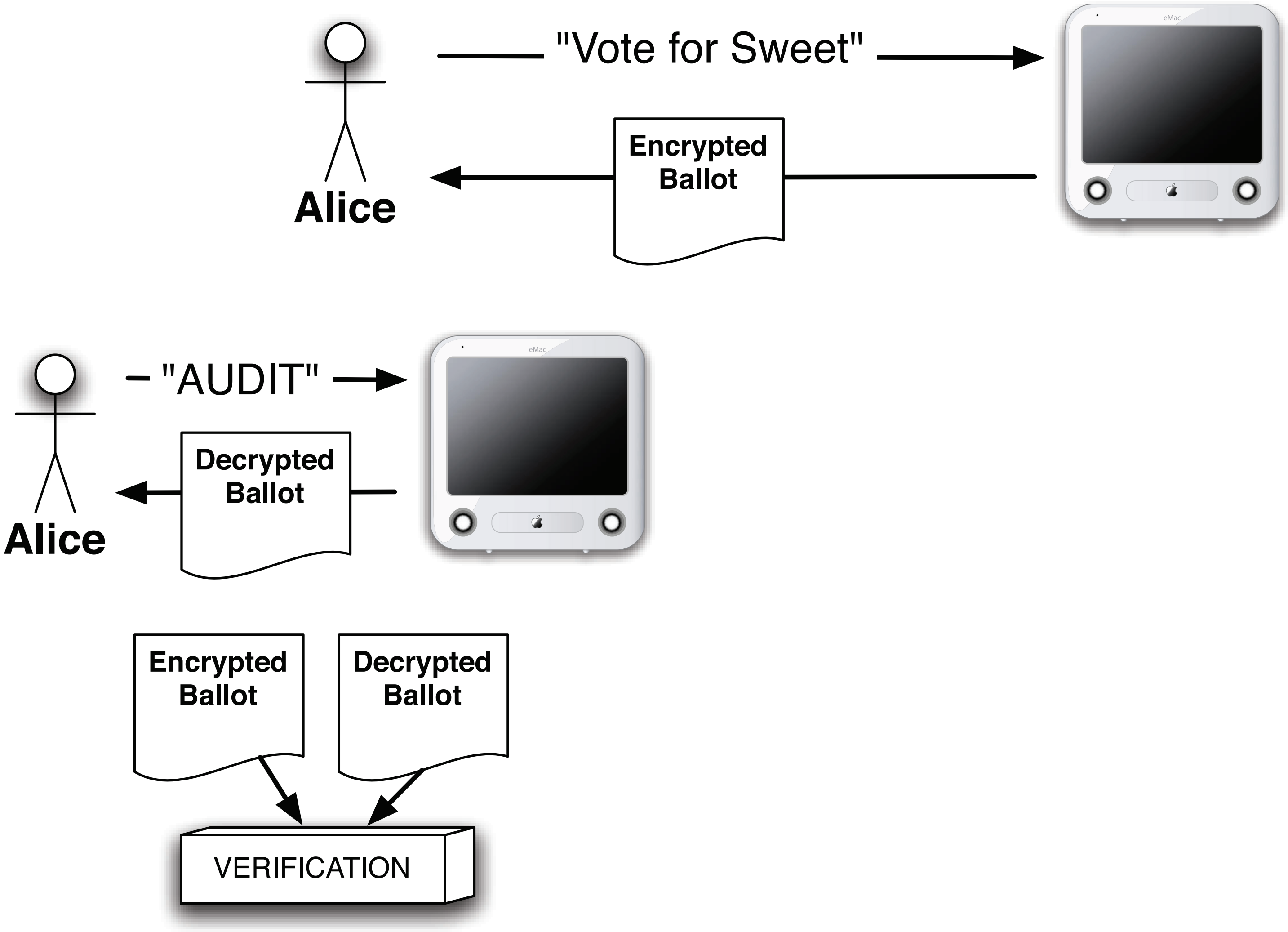
Alice

"AUDIT"

Decrypted Ballot

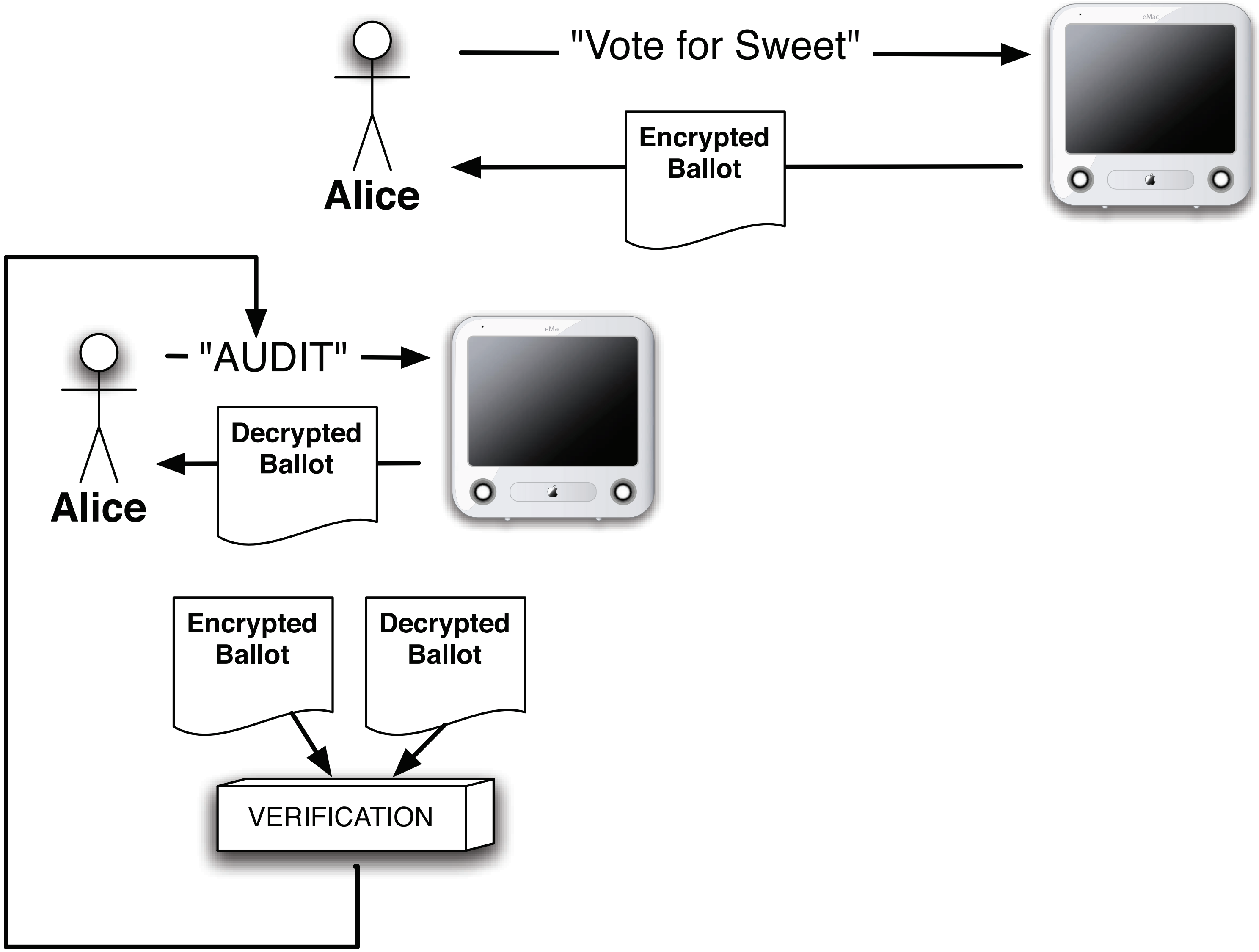
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



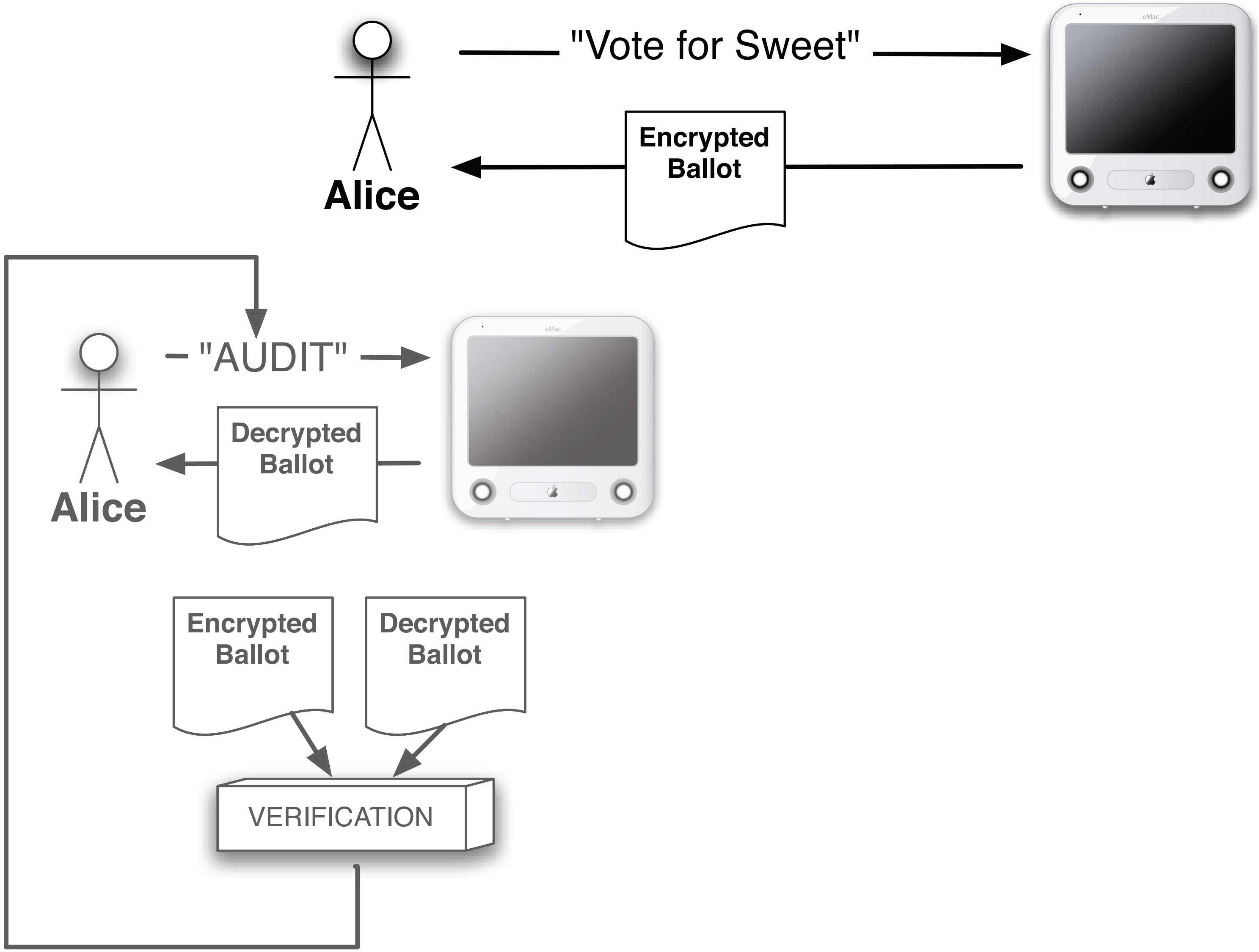
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



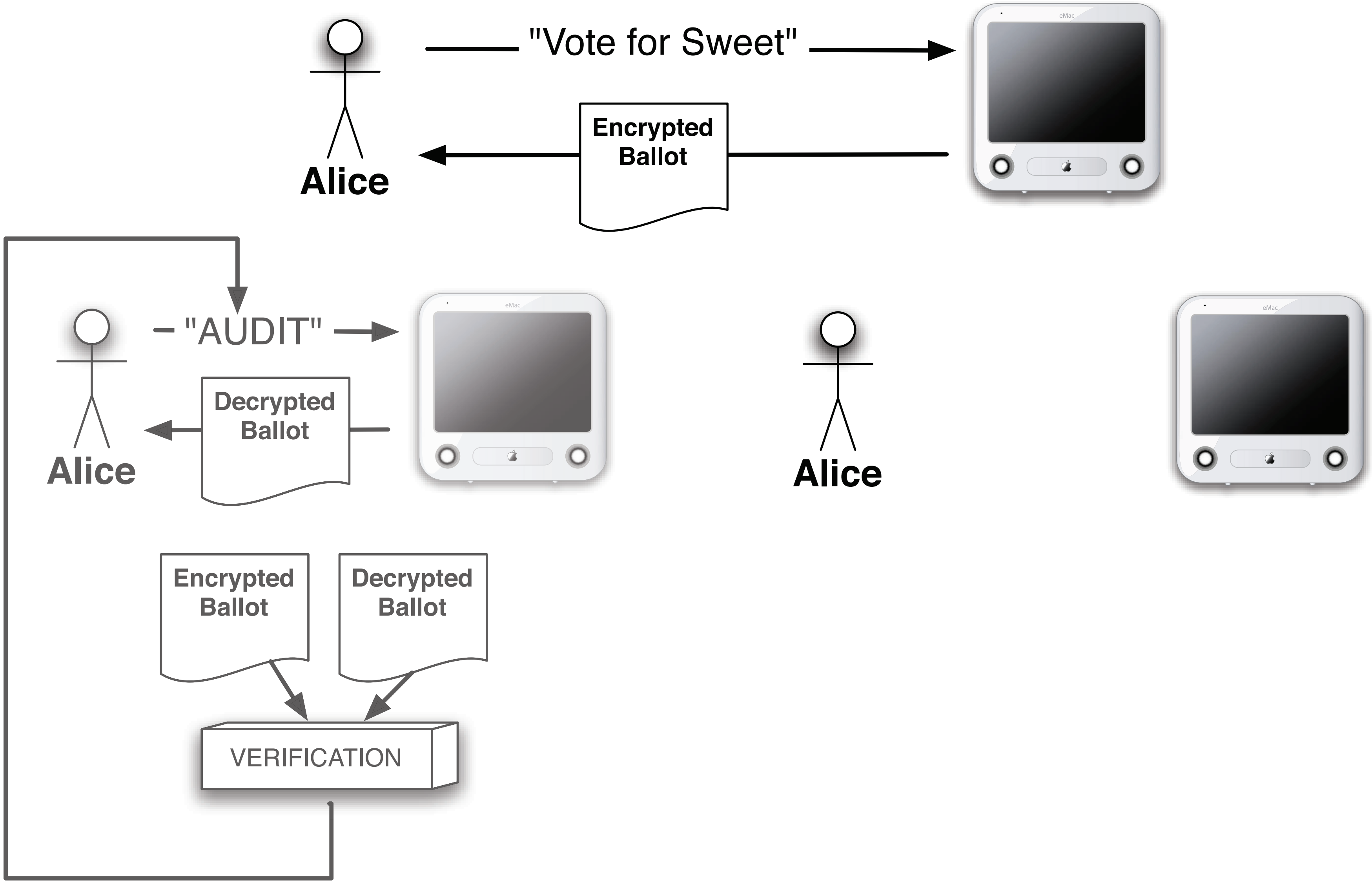
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



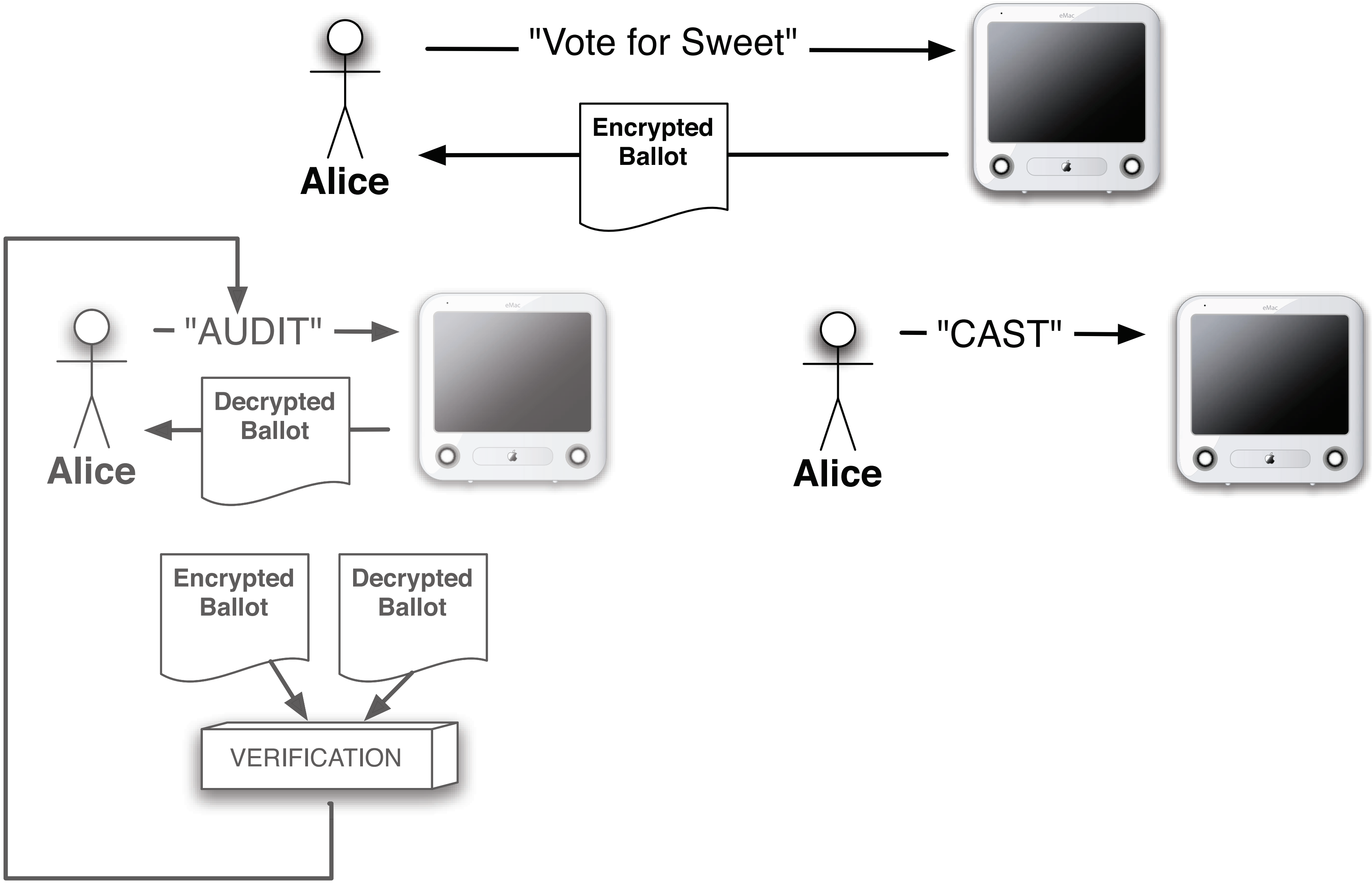
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



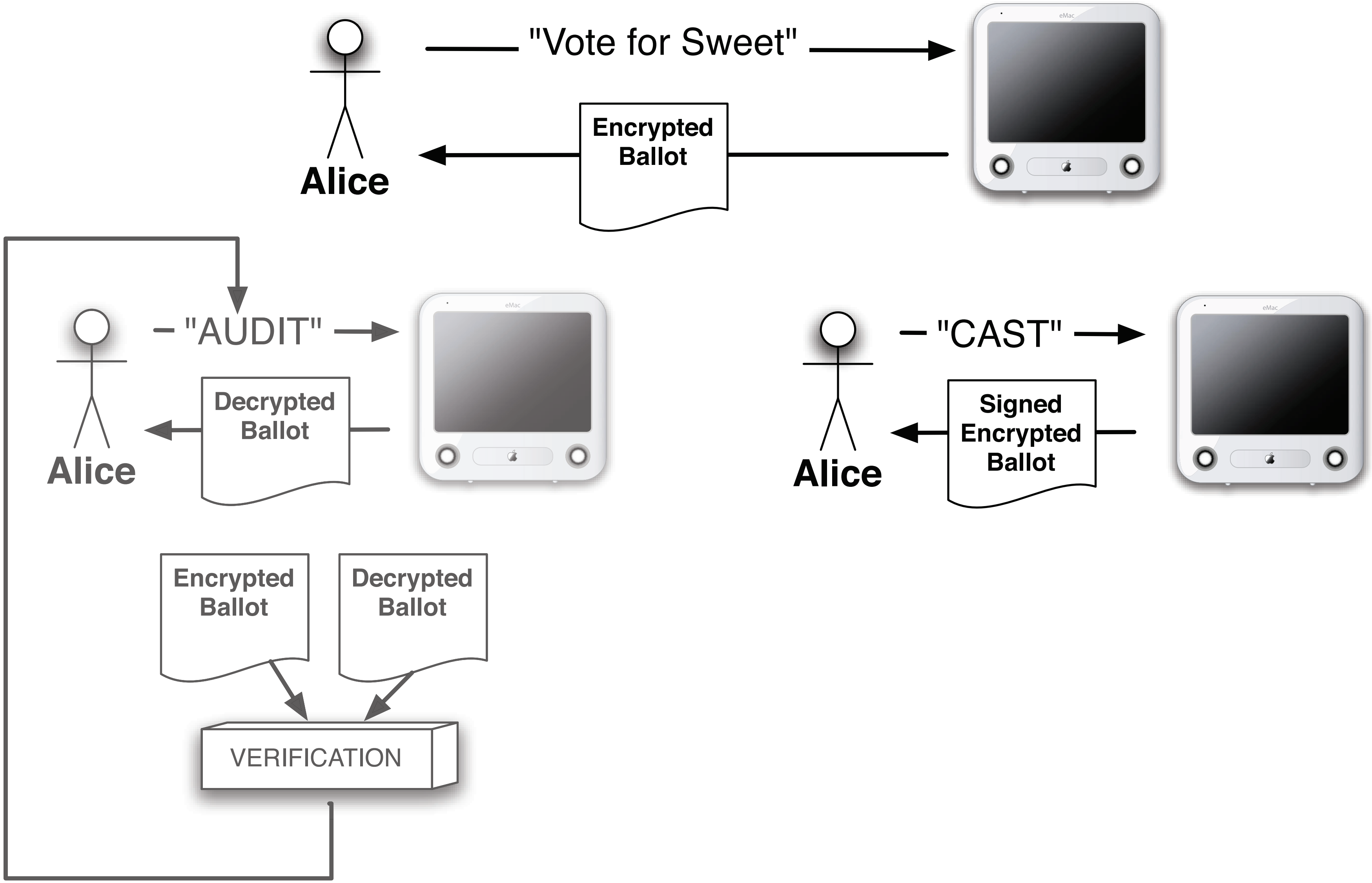
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



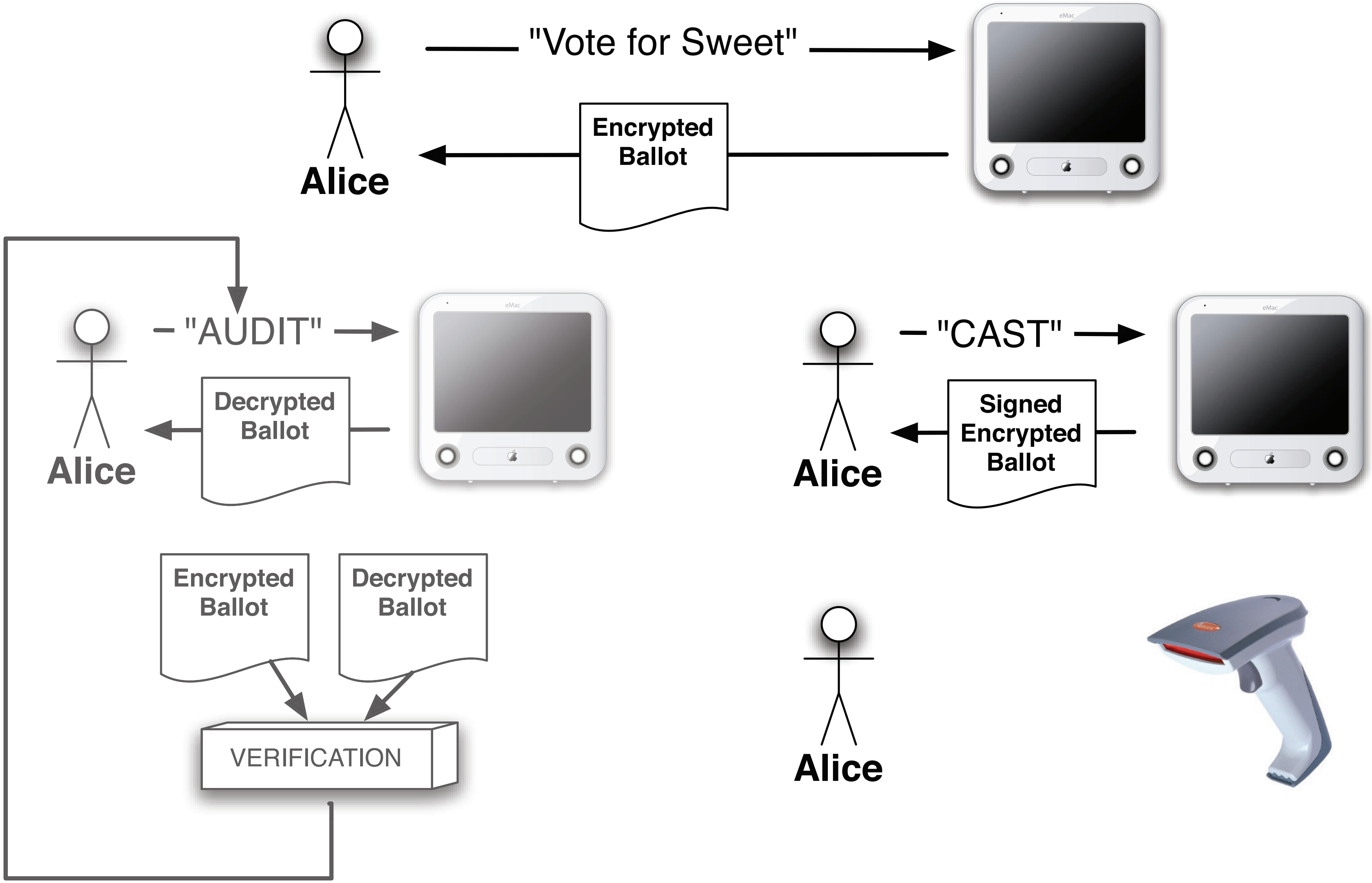
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Verifying Consistency [Benaloh]



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

Verifying Consistency [Benaloh]



Alice

"Vote for Sweet"

Encrypted Ballot

Alice

"AUDIT"

Decrypted Ballot

Encrypted Ballot

Decrypted Ballot

VERIFICATION

Alice

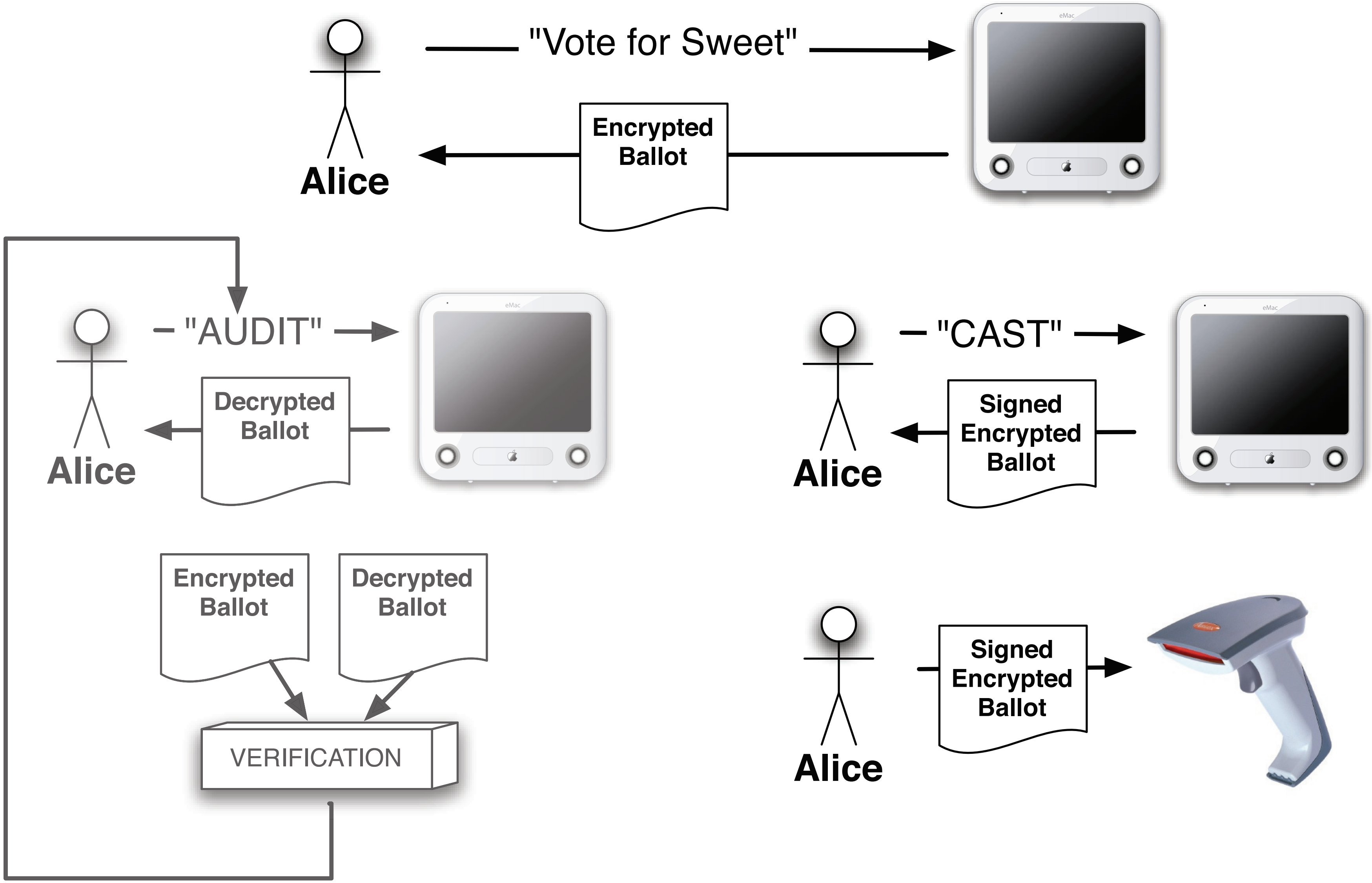
"CAST"

Signed Encrypted Ballot

Alice

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

Verifying Consistency [Benaloh]



Alice

"Vote for Sweet"

Encrypted Ballot

Alice

"AUDIT"

Decrypted Ballot

Encrypted Ballot

Decrypted Ballot

VERIFICATION

Alice

"CAST"

Signed Encrypted Ballot

Alice

Signed Encrypted Ballot

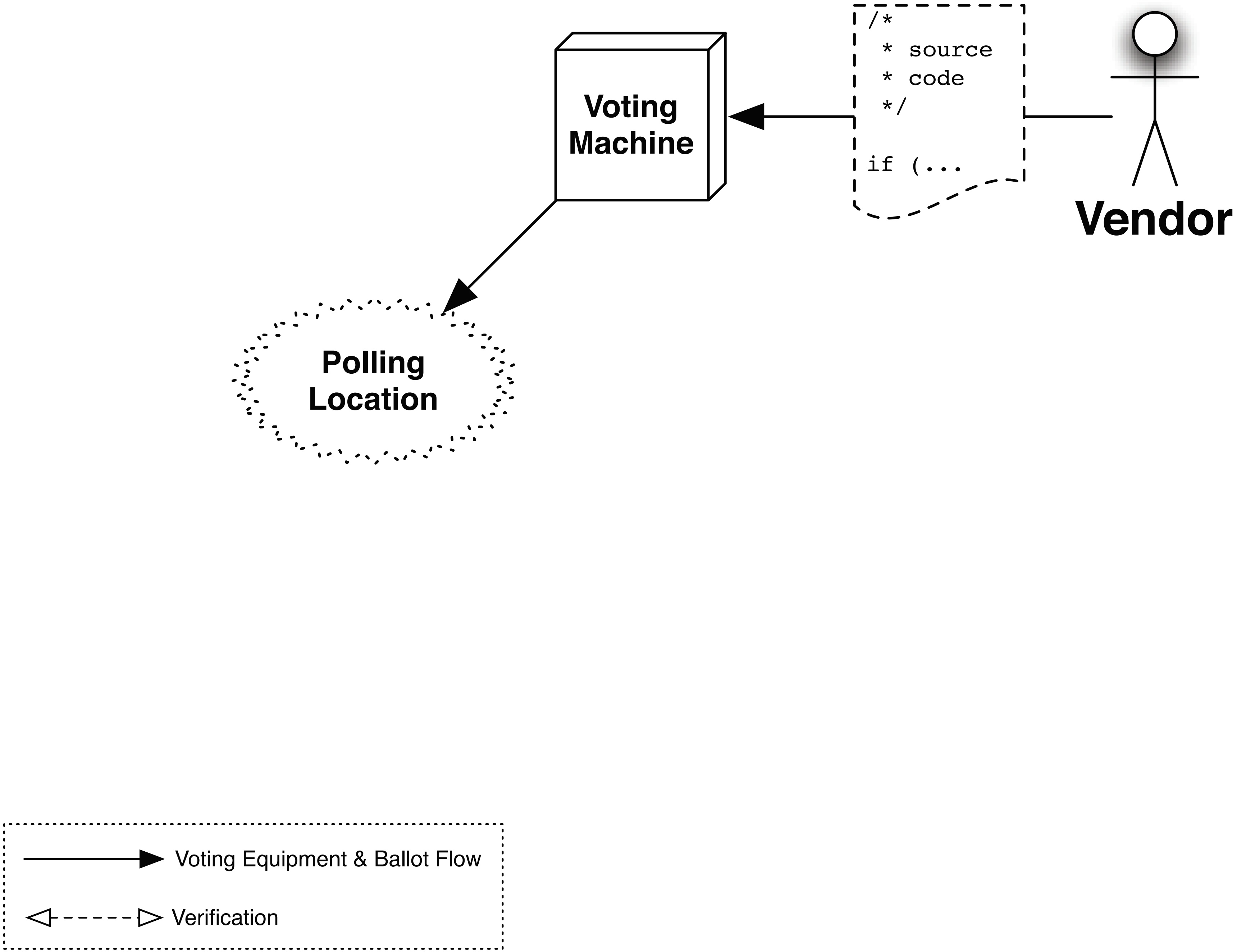
http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg

Putting It Together

——▶ Voting Equipment & Ballot Flow

◁- - - - -▷ Verification

Putting It Together



Voting Machine

```
/*
 * source
 * code
 */

if (...
```

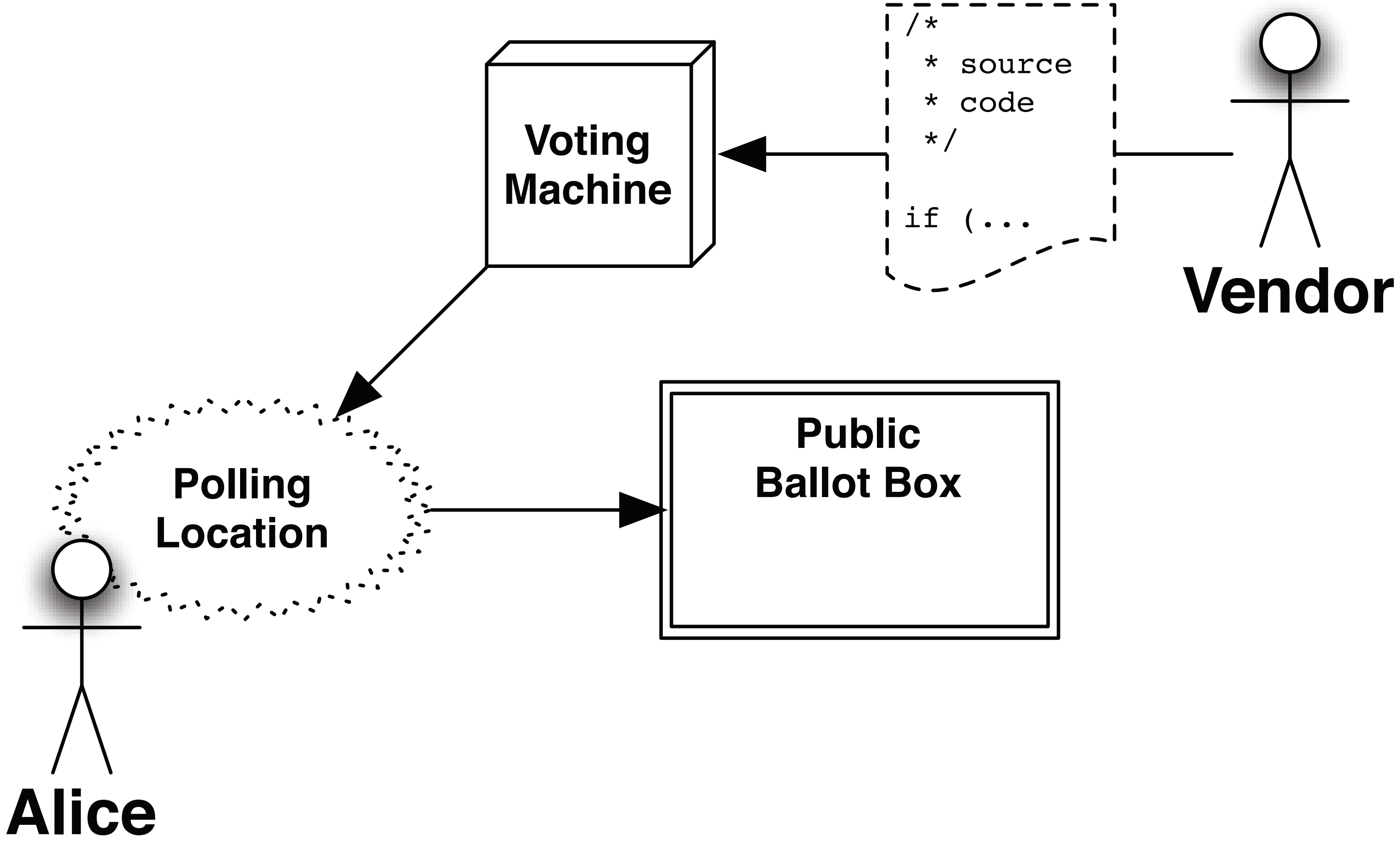
Vendor

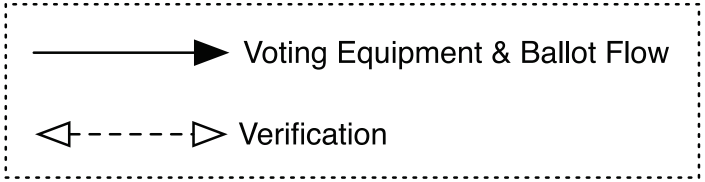
Polling Location

Voting Equipment & Ballot Flow

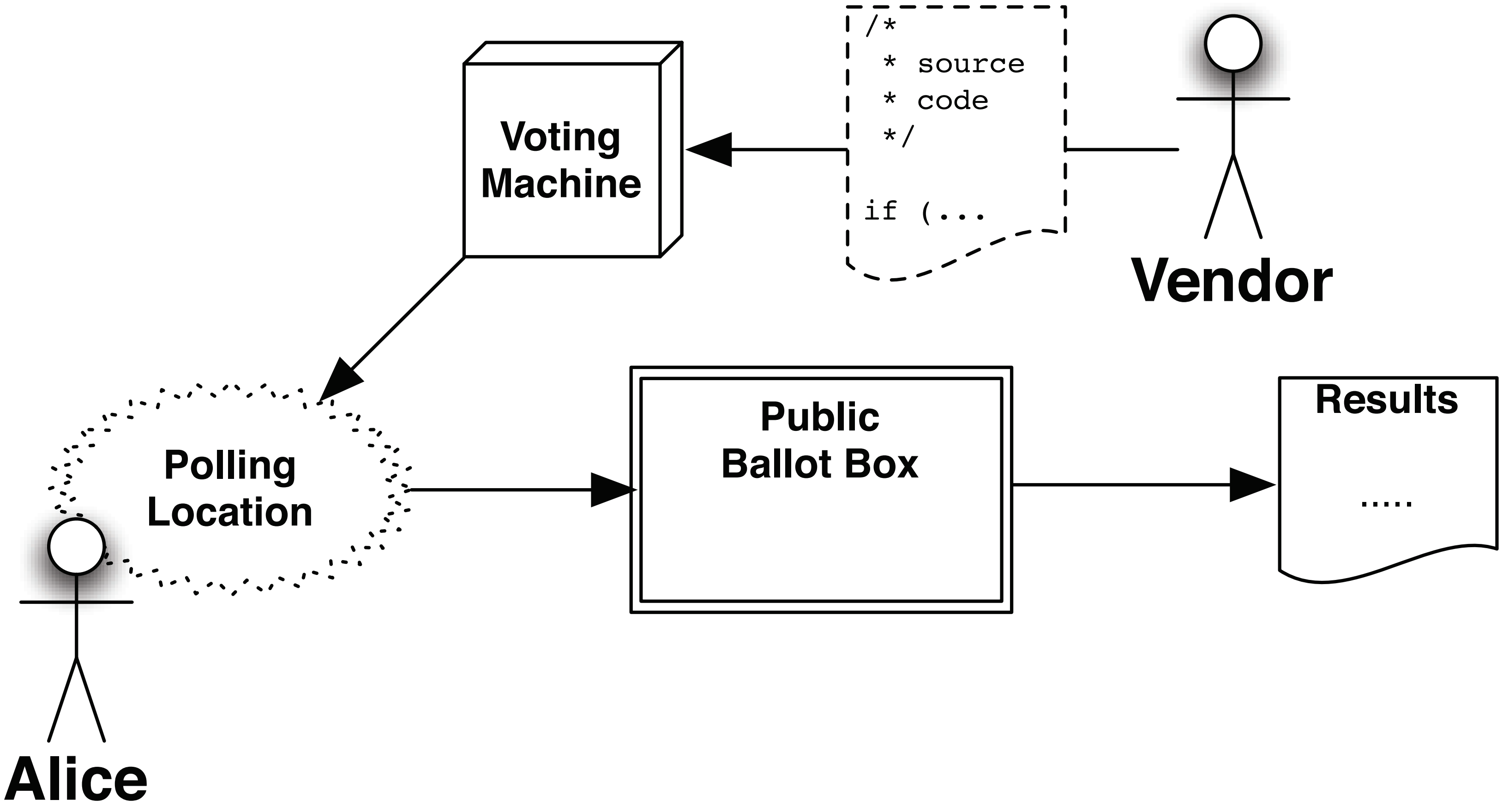
Verification

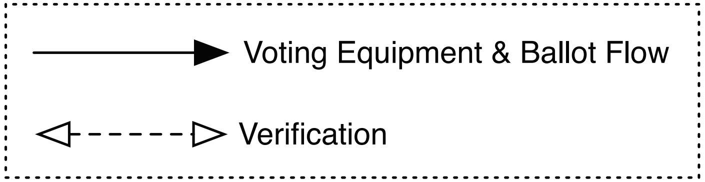
Putting It Together



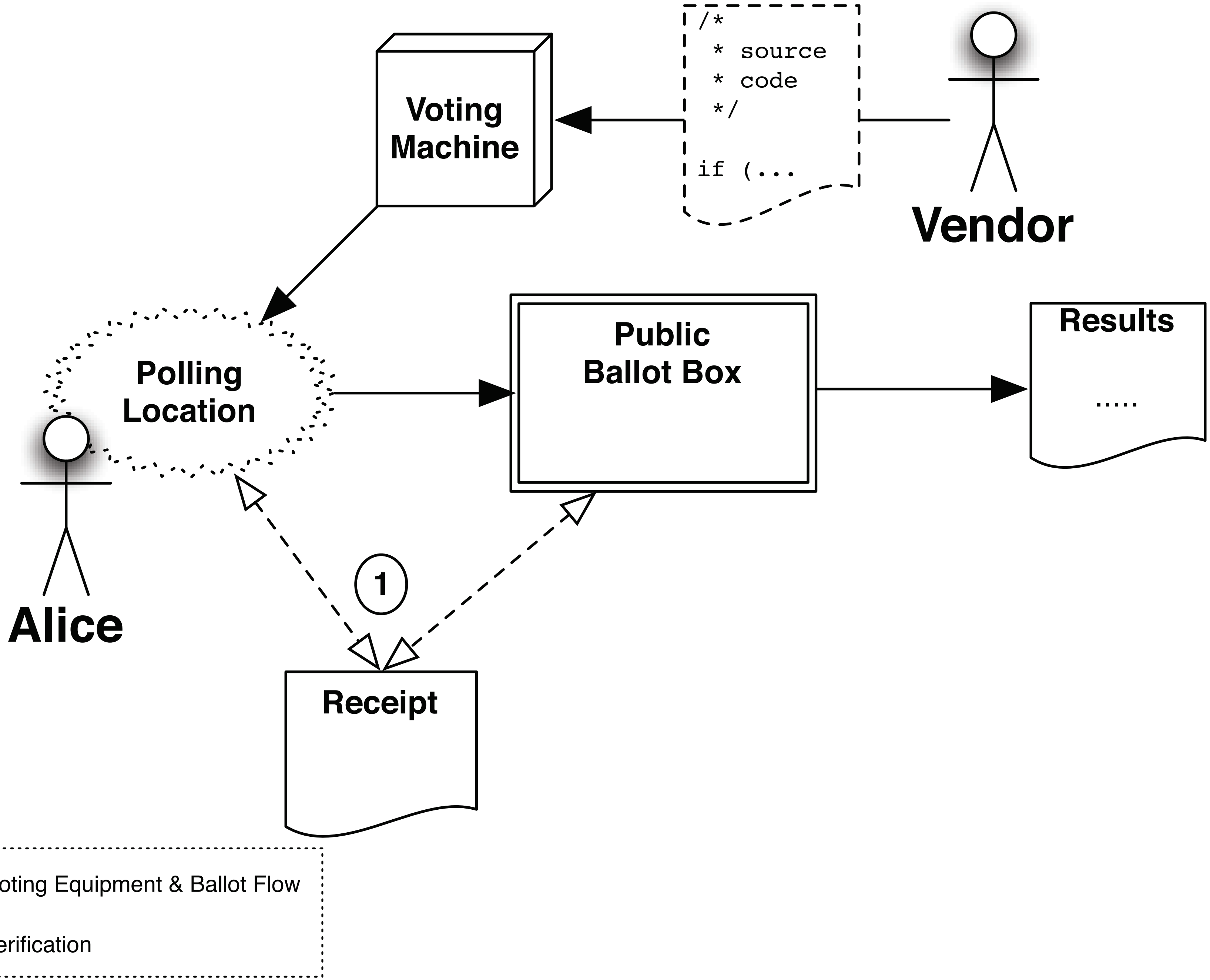


Putting It Together

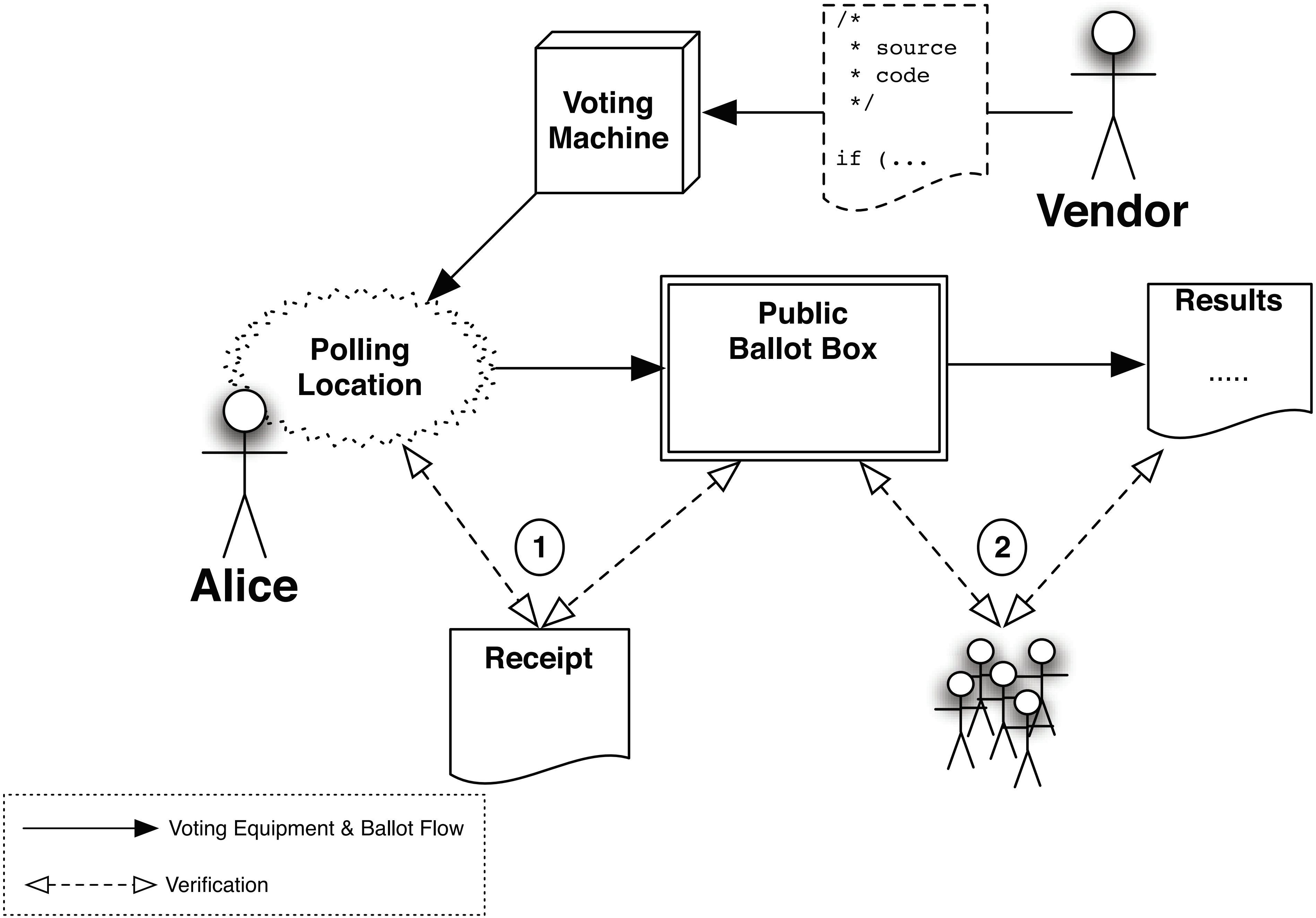




Putting It Together



Putting It Together



Voting Machine

```
/*
 * source
 * code
 */

if (...
```

Vendor

Polling Location

Public Ballot Box

Results

.....

Alice

1

2

Receipt

Voting Equipment & Ballot Flow

Verification

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.

Questions?