

Open-Audit Elections

Ben Adida

Harvard

(novel work done at MIT, in collaboration with Ronald L. Rivest)

Google

November 16th, 2006

Lloyd Bentsen

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: Oct

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: Oct

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: Oct

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: Oct

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](#)

Reporter

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine

Does e-voting need paper trails?

By Anne Broache

Staff Writer,

Published: Oct

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

Reporter

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

Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

Thief grabs voting machine from election official's car

By ROGER H. AYLWORTH - Staff Writer

Article Launched: 11/07/2006 12:00:00 AM PST

Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

Thief grabs voting machine from election official's car

By ROGER H. AYLWORTH - Staff Writer

Article Launched: 11/07/2006 12:00:00 AM PST

Last Updated: November 7, 2006 - 2:19 PM EST

Voter smashes touch-screen machine in Allentown

Rodgers precinct with more than 100 percent
VO

**The
off**
By R
Artic



Last Updated: November 7, 2006 - 2:19 PM EST

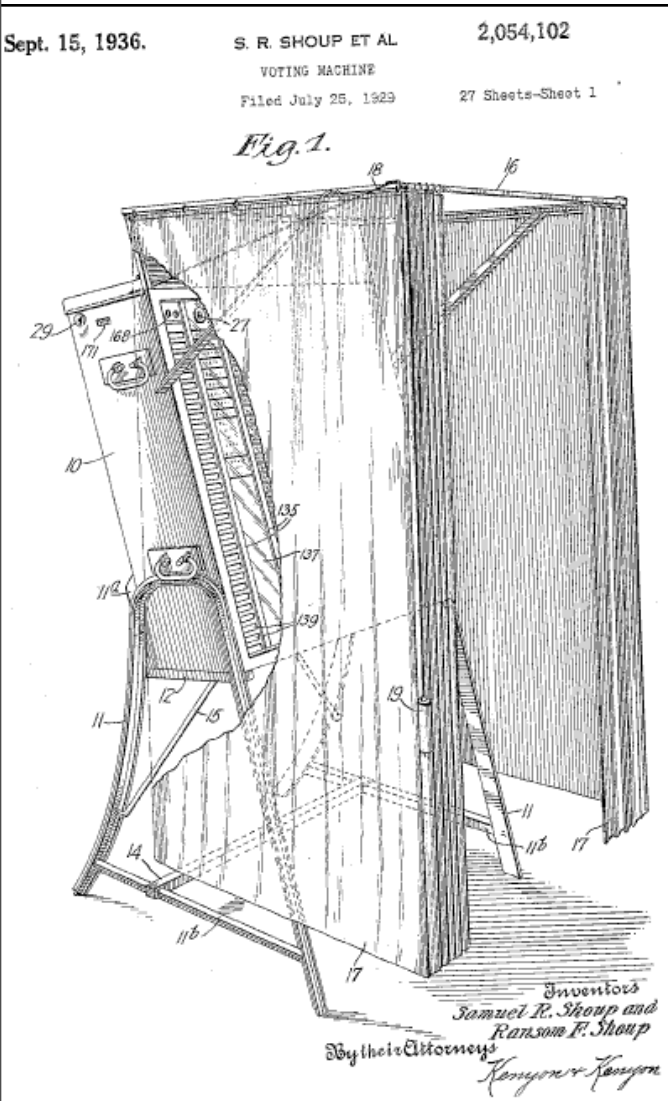
**Voter smashes touch-screen machine in
Allentown**

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 a local bar.

How We Got Here

How We Got Here



How We Got Here

Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102
VOTING MACHINE
Filed July 25, 1929 27 Sheets-Sheet 1

DO NOT DETACH STUB-FOLD OVER

1	40	97	117	136	156	176	196	216
2	21	59	78	98	118	137	157	177
3	22	41	79	99	119	138	158	178
4	23	42	60	80	100	139	159	179
5	24	43	61	81	101	140	160	180
6	25	44	62	82	102	141	161	181
7	26	45	63	83	103	142	162	182
8	27	46	64	84	104	143	163	183
9	28	47	65	85	105	144	164	184
10	29	48	66	86	106	145	165	185
11	30	49	67	87	107	146	166	186
12	31	50	68	88	108	147	167	187
13	32	51	69	89	109	148	168	188
14	33	52	70	90	110	149	169	189
15	34	53	71	91	111	150	170	190
16	35	54	72	92	112	151	171	191
17	36	55	73	93	113	152	172	192
18	37	56	74	94	114	153	173	193
19	38	57	75	95	115	154	174	194
20	39	58	76	96	116	155	175	195

TO BE FILLED IN BY COUNTING BOARD ONLY
PRECINCT NO. WRITE-IN NO.

How We Got Here

Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102
VOTING MACHINE
Filed July 25, 1929 27 Sheets-Sheet 1

DO NOT DETACH STUB-FOLD OVER

1	40	97	117	136	156	176	196	216
2	21	59	78	98	118	137	157	177
3	22	41	79	99	119	138	158	178
4	23	42	60	80	100	120	139	159
5	24	43	61	81	101	121	140	160
6	25	44	62	82	102	122	141	161
7	26	45	63	83	103	123	142	162
8	27	46	64	84	104	124	143	163
9	28	47	65	85	105	125	144	164
10	29	48	66	86	106	126	145	165
11	30	49	67	87	107	127	146	166
12	31	50	68	88	108	128	147	167
13	32	51	69	89	109	129	148	168
14	33	52	70	90	110	130	149	169
15	34	53	71	91	111	131	150	170
16	35	54	72	92	112	132	151	171
17	36	55	73	93	113	133	152	172
18	37	56	74	94	114	134	153	173
19	38	57	75	95	115	135	154	174
20	39	58	76	96	116	136	155	175

TO BE FILLED IN BY COUNTING BOARD ONLY
PRECINCT NO. WRITE-IN NO.

How We Got Here

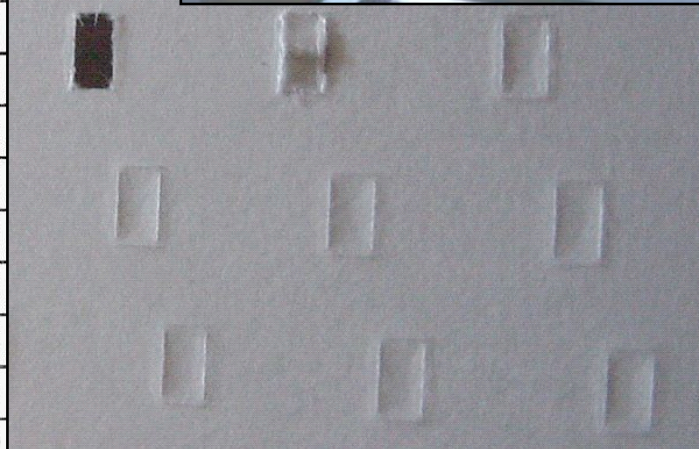
Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102

VOTING MACHINE
Filed July 25, 1929 27

DO NOT DETACH STUD

1	40	97	117
2	21	59	78
3	22	41	98
4	23	60	79
5	24	61	99
6	25	80	119
7	26	81	100
8	27	82	120
9	28	83	101
10	29	84	121
11	30	85	102
12	31	86	122
13	32	87	103
14	33	88	123
15	34	89	104
16	35	90	124
17	36	91	
18	37	92	
19	38	93	
20	39	94	

TO BE FILLED IN BY COUNTING BOARD ONLY
PRECINCT NO. WRITE-IN NO.



How We Got Here

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

VOTING MACHINE
Filed July 25, 1929 27

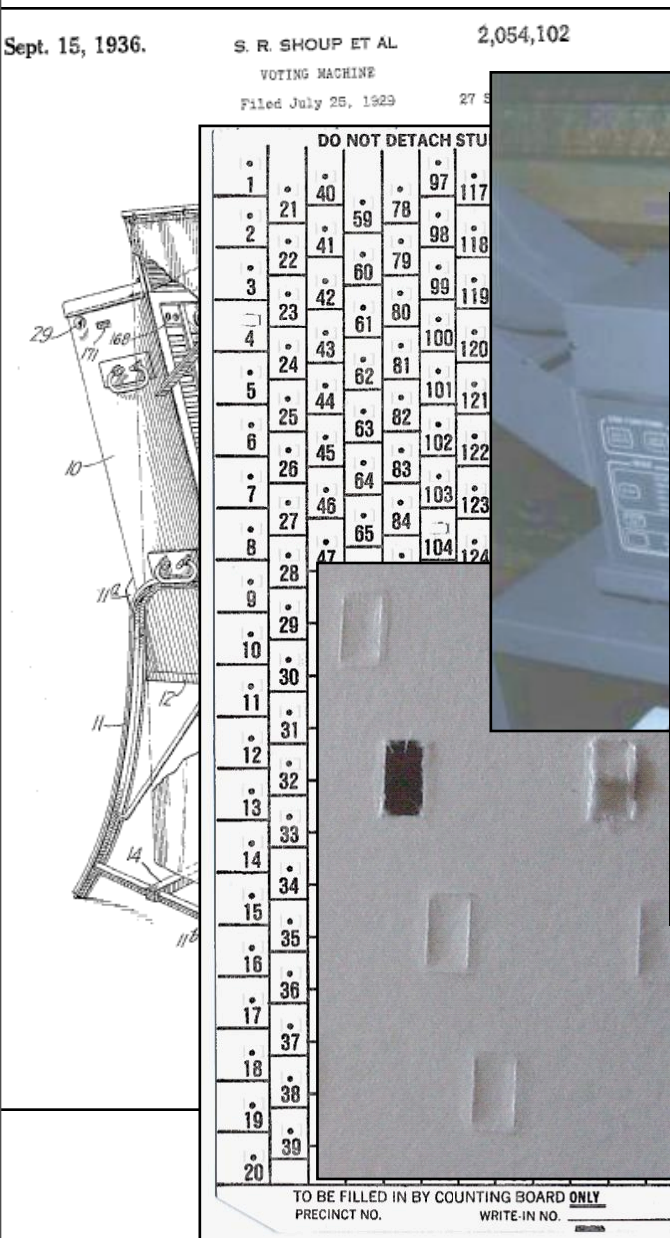
DO NOT DETACH STUD

1	40	97	117
2	21	59	78
3	22	41	98
4	23	60	79
5	24	61	99
6	25	80	119
7	26	81	100
8	27	82	120
9	28	83	101
10	29	84	121
11	30	85	102
12	31	103	122
13	32	104	123
14	33		124
15	34		
16	35		
17	36		
18	37		
19	38		
20	39		

TO BE FILLED IN BY COUNTING BOARD ONLY
PRECINCT NO. _____ WRITE-IN NO. _____



How We Got Here



2 Months Ago: Princeton Report

The screenshot shows a software interface titled "VOTE STEALING CONTROL PANEL". It includes a dropdown menu for selecting a race, a table of candidates with their current vote counts and percentages, a slider for setting the final outcome for a specific candidate, and "OK" and "Cancel" buttons at the bottom.

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%

OK Cancel

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

[FHF2006]

But not just DREs...

State of Connecticut
Official Absentee Ballot

Town of Westport, Connecticut Municipal Election Test Election Sheet 1 of 2

Be sure to read instructions on reverse side of this ballot.

	1	2	3	4	5	6	7	8	9	10	11	12
OFFICE	Board of Finance Vote for Any Four				Board of Education Vote for Any Three			Board of Assessment Appeals	Planning and Zoning Commission Vote for Any Four			
PARTY												
REPUBLICAN	<input checked="" type="radio"/> 1A R. Gavin S. Anderson	<input type="radio"/> 2A Thomas C. Brook	<input checked="" type="radio"/> 3A Ralph Hymans	<input checked="" type="radio"/> 4A Charles W.K. Haberbach	<input type="radio"/> 5A Edward M. Bowers	<input type="radio"/> 6A Lewin D. Brey	<input type="radio"/> 7A Gordon F. Weller, Jr.	<input checked="" type="radio"/> 8A Shan M. Timmons	<input type="radio"/> 9A Helen Martha Block	<input checked="" type="radio"/> 10A James R. Eckhardt	<input type="radio"/> 11A David S. Prest	<input type="radio"/> 12A
DEMOCRATIC	<input type="radio"/> 1B Steven L. Ezra	<input checked="" type="radio"/> 2B Kevin A. Connolly	<input type="radio"/> 3B	<input type="radio"/> 4B	<input checked="" type="radio"/> 5B Mark H. Mathias	<input type="radio"/> 6B Mary R. Parnell	<input type="radio"/> 7B	<input type="radio"/> 8B	<input checked="" type="radio"/> 9B Eleanor S. Lowenthal	<input type="radio"/> 10B	<input type="radio"/> 11B	<input type="radio"/> 12B
SAVE WESTPORT NOW	<input type="radio"/> 1C	<input type="radio"/> 2C	<input type="radio"/> 3C	<input type="radio"/> 4C	<input type="radio"/> 5C	<input type="radio"/> 6C	<input type="radio"/> 7C	<input type="radio"/> 8C	<input checked="" type="radio"/> 9C Eleanor S. Lowenthal	<input type="radio"/> 10C	<input type="radio"/> 11C	<input type="radio"/> 12C
PETITIONING CANDIDATE	<input type="radio"/> 1D	<input type="radio"/> 2D	<input type="radio"/> 3D	<input type="radio"/> 4D	<input type="radio"/> 5D Stephen M. Rubin	<input type="radio"/> 6D Robert Hain Andrew	<input checked="" type="radio"/> 7D Robert M. Chase	<input type="radio"/> 8D	<input type="radio"/> 9D	<input type="radio"/> 10D	<input type="radio"/> 11D	<input type="radio"/> 12D
WRITE-IN VOTES	<input type="radio"/> 1F	<input type="radio"/> 2F	<input type="radio"/> 3F	<input type="radio"/> 4F	<input type="radio"/> 5F	<input type="radio"/> 6F	<input type="radio"/> 7F	<input type="radio"/> 8F	<input type="radio"/> 9F	<input type="radio"/> 10F	<input type="radio"/> 11F	<input type="radio"/> 12F

[KMRS2006]

We can do better

Beyond DREs and Paper Trails,
there is a *third option*:
open-audit elections

Direct, end-to-end verification by voter.
No need to trust equipment.

Let's talk about it.

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!”

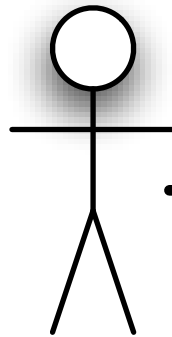
Dick Tuck
1966 Concession Speech

Provide enough evidence
to convince the loser.

Secret Ballot vs. Verifiability

Voting System

convince



Alice



Carl the Coercer



1892 - Australian Ballot

1893

<input type="radio"/> DEMOCRATIC.	<input type="radio"/> REPUBLICAN.
<input type="checkbox"/> FOR MAYOR, AUGUST LEUZ, JR. CORNER BURLINGTON AND JOHNSON STREETS.	<input type="checkbox"/> FOR MAYOR, CHAS. LEWIS <i>Majorities</i> 221 NO. 227 NORTH CLINTON STREET.
<input type="checkbox"/> FOR TREASURER, GEORGE W. KOONTZ 848 NO. 620 EAST BURLINGTON STREET.	<input type="checkbox"/> FOR TREASURER,
<input type="checkbox"/> FOR CITY SOLICITOR, FRANK J. HORAK NO. 120 DODGE STREET.	<input type="checkbox"/> FOR SOLICITOR, L. H. FULLER 101 NO. 422 SOUTH DUBUQUE STREET.
<input type="checkbox"/> FOR ASSESSOR, F. A. HEINSIUS NO. 948 EAST MARKET STREET.	<input type="checkbox"/> FOR ASSESSOR, H. W. LATHROP 198 NO. 518 IOWA AVENUE.
FOURTH WARD.	FOURTH WARD.
<input type="checkbox"/> FOR TRUSTEE, JOHN U. MILLER 24 EAST MARKET STREET.	<input type="checkbox"/> FOR TRUSTEE, J. C. LEASURE COR. VAN BUREN ST. AND IOWA AVENUE.

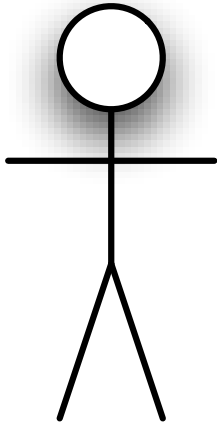
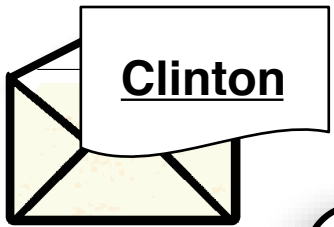
The Next Harvard Prez!

SOURCES: HARVARD WANTS
CONDOLEEZZA RICE OR BILL
CLINTON FOR NEXT PRES...

US News & World Report/Washington Whispers | Paul Bedard | Posted September 10, 2006 02:43 PM

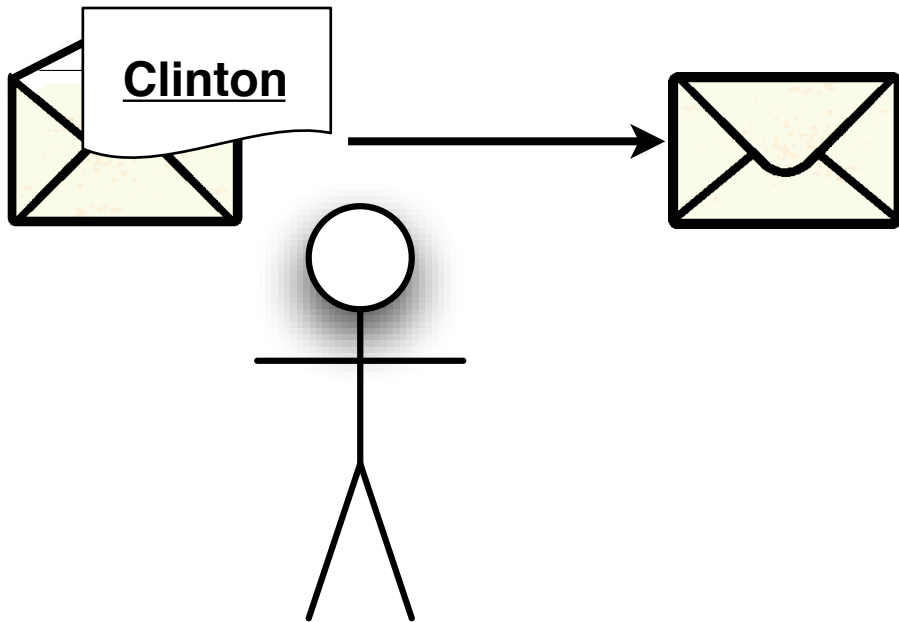


The Ballot Handoff



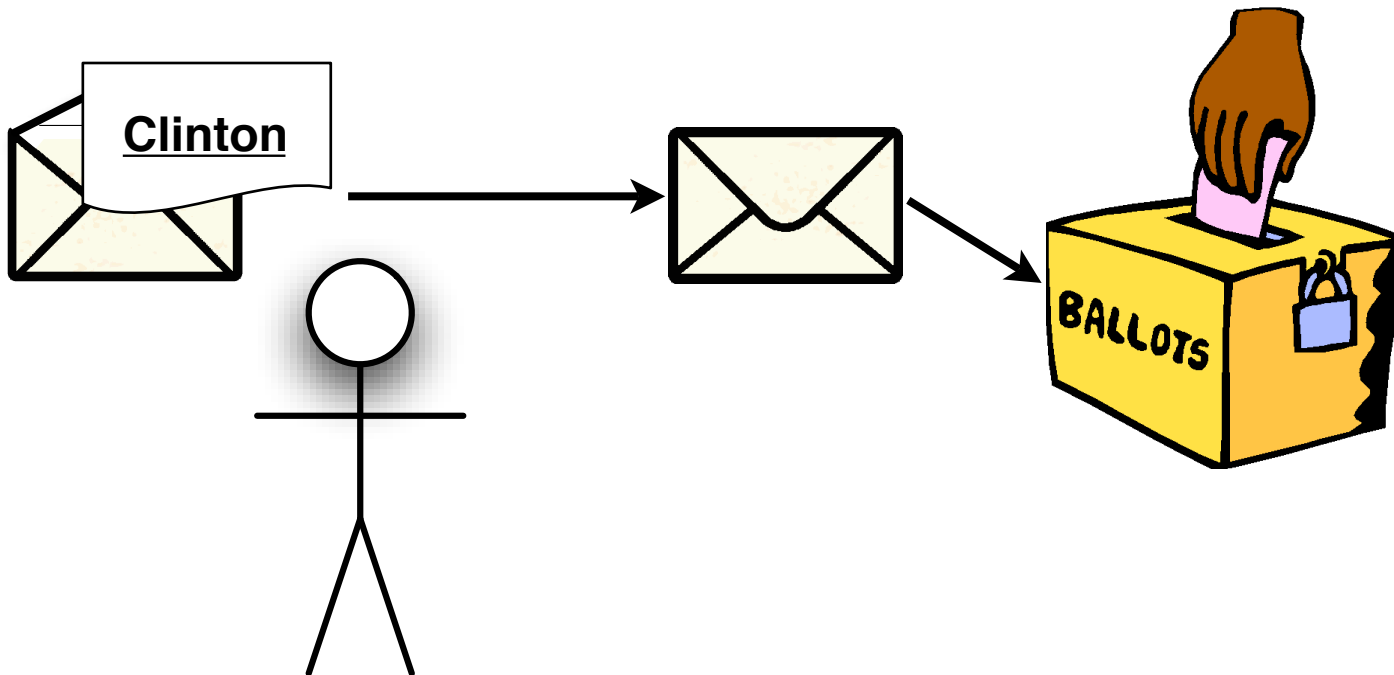
Alice the Voter

The Ballot Handoff



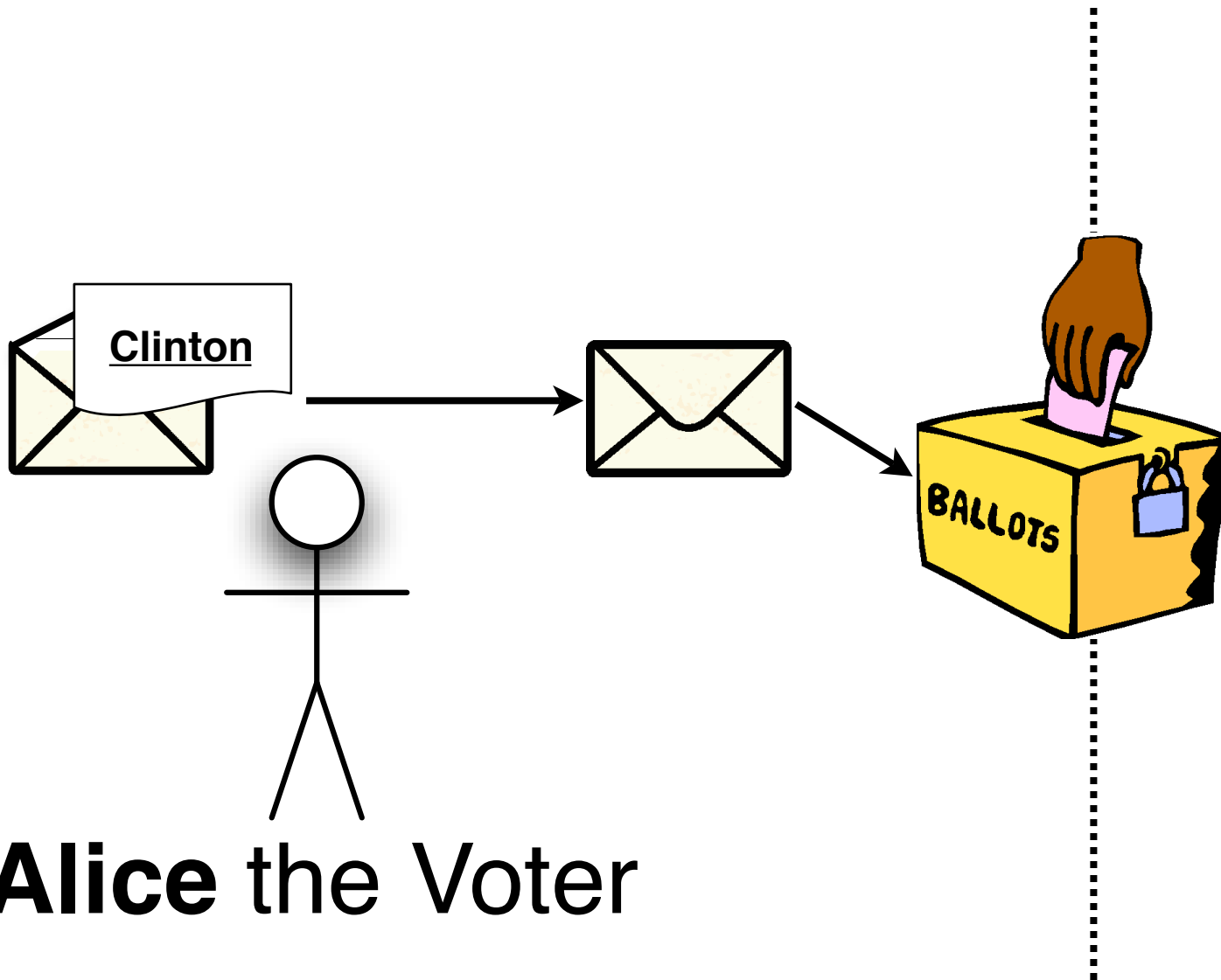
Alice the Voter

The Ballot Handoff



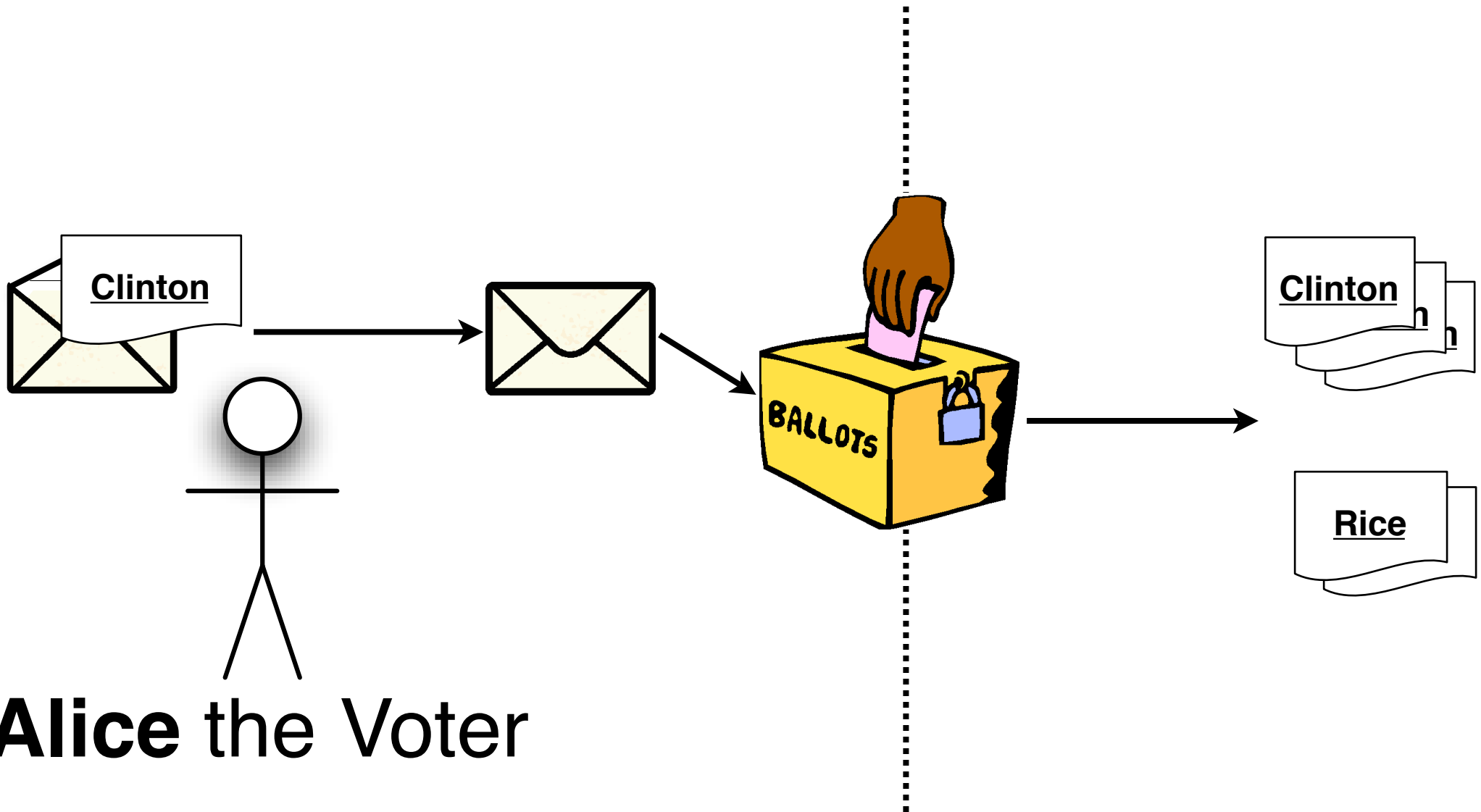
Alice the Voter

The Ballot Handoff

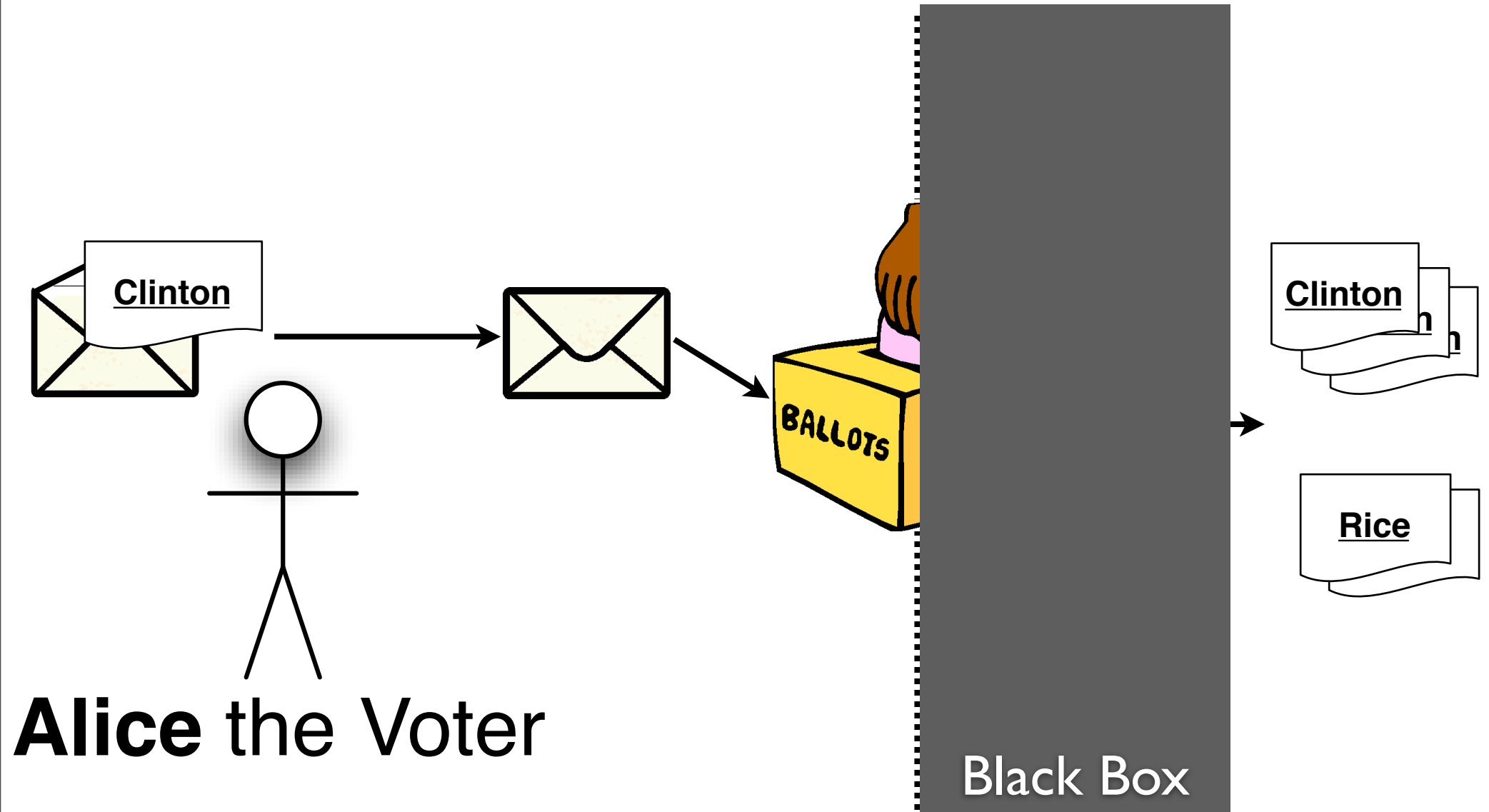


Alice the Voter

The Ballot Handoff

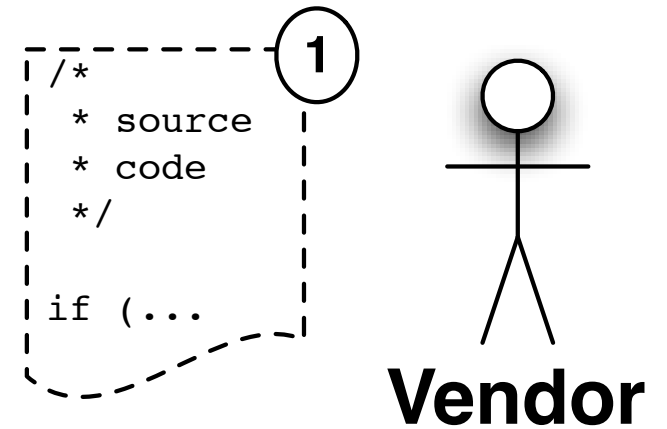


The Ballot Handoff

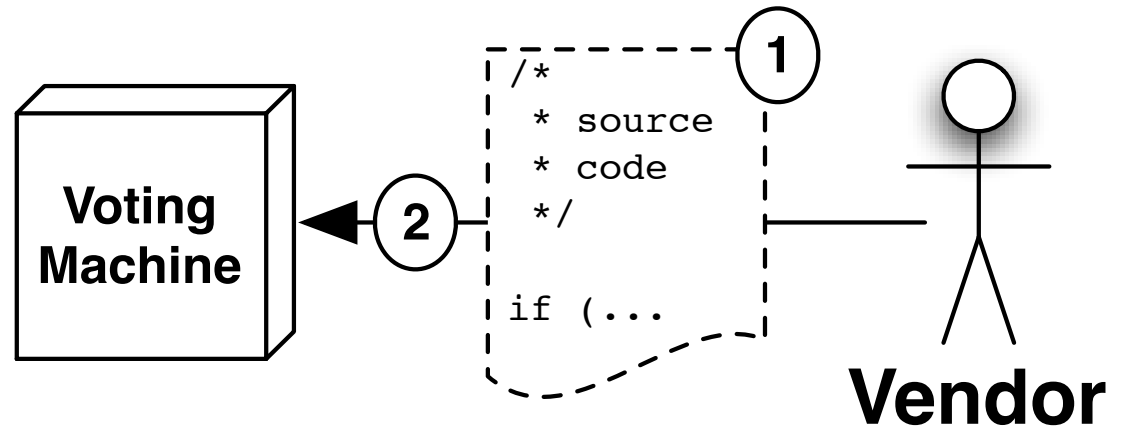


Chain of Custody

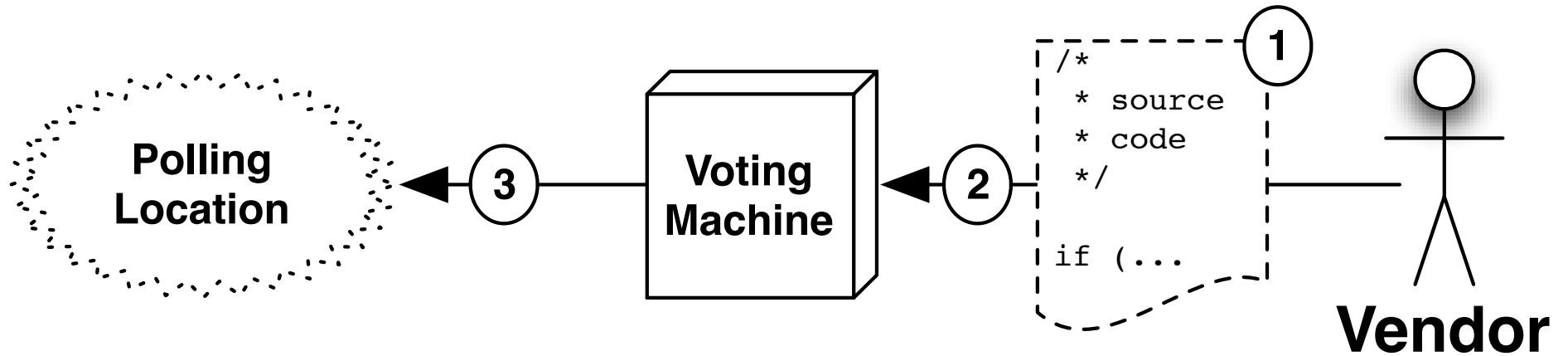
Chain of Custody



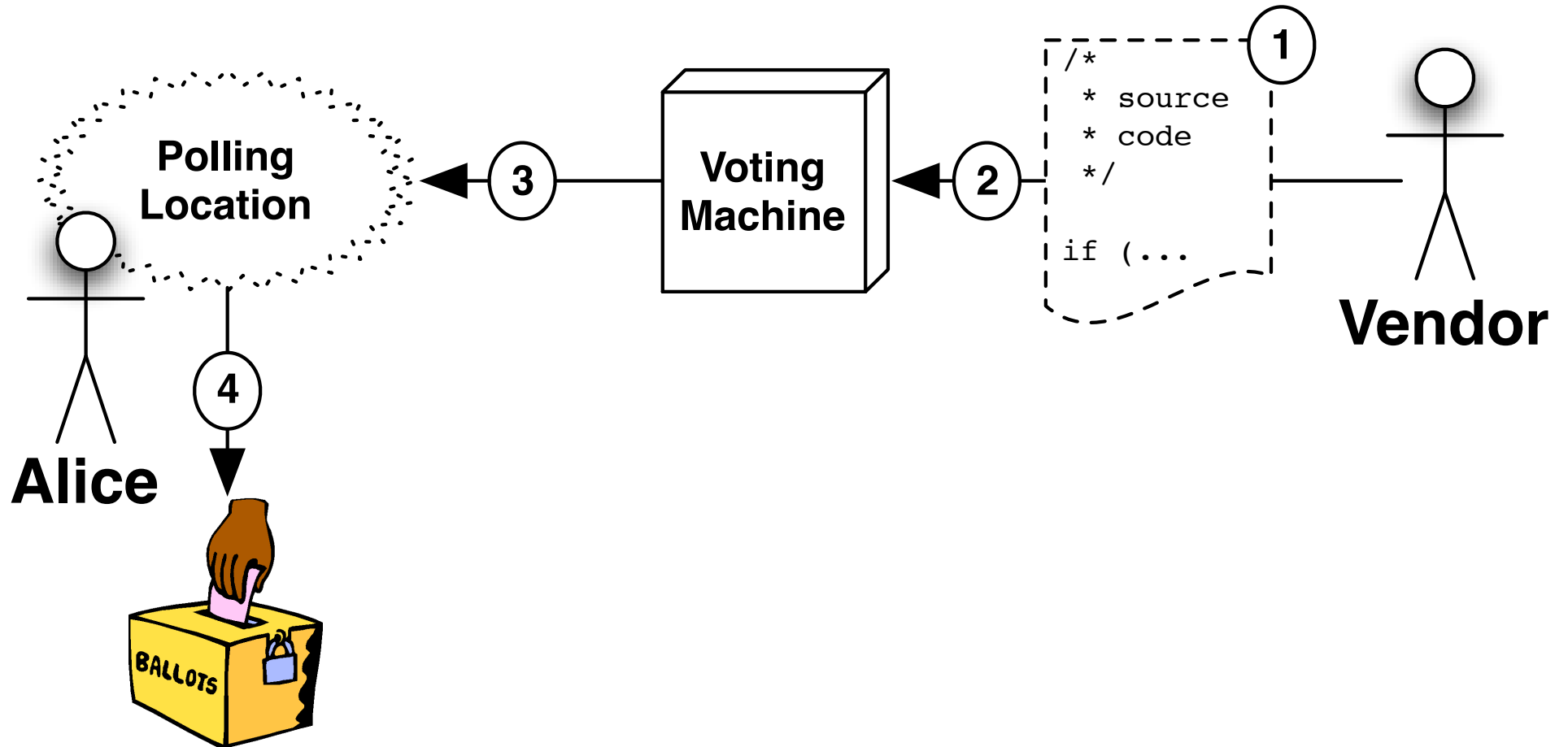
Chain of Custody



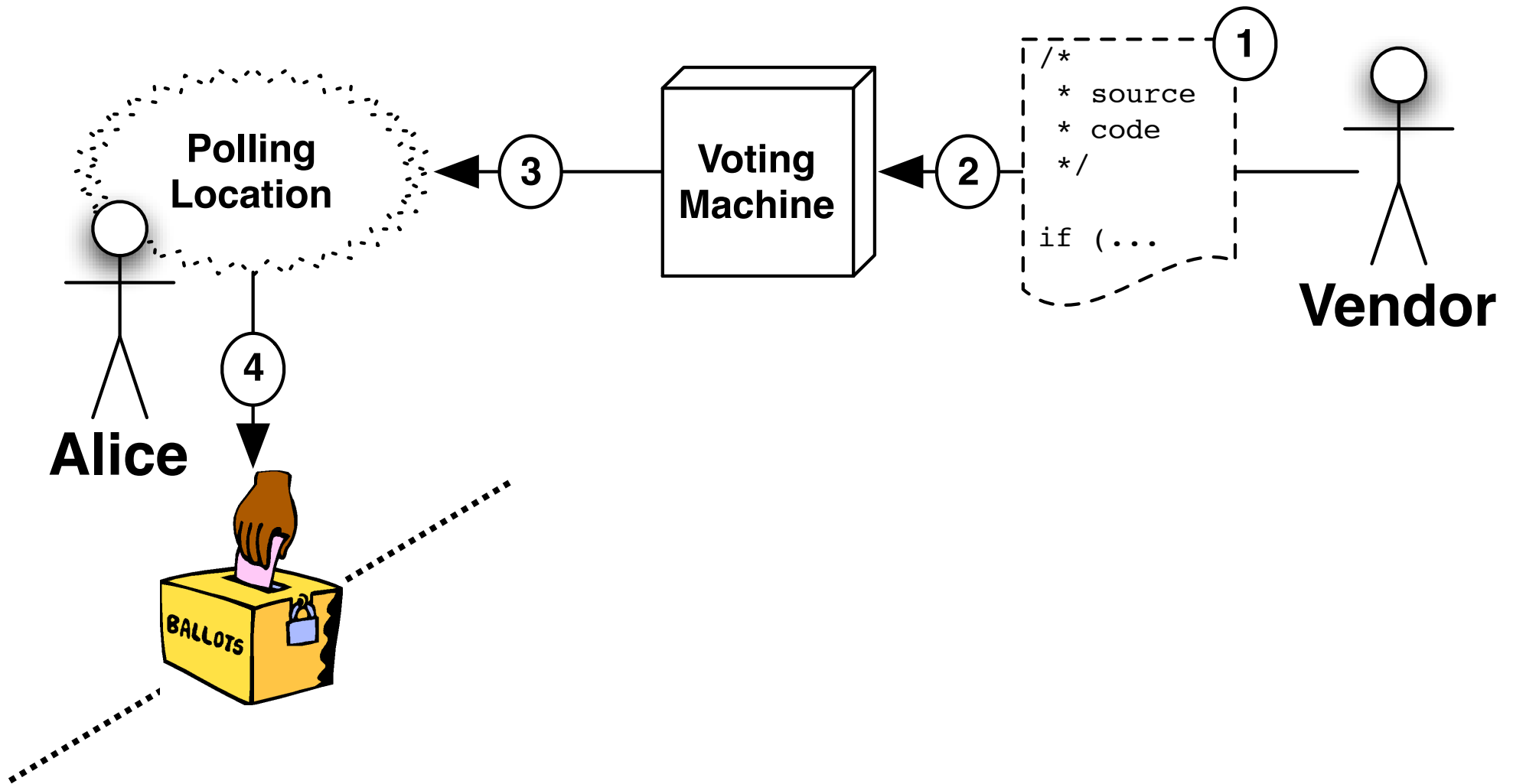
Chain of Custody



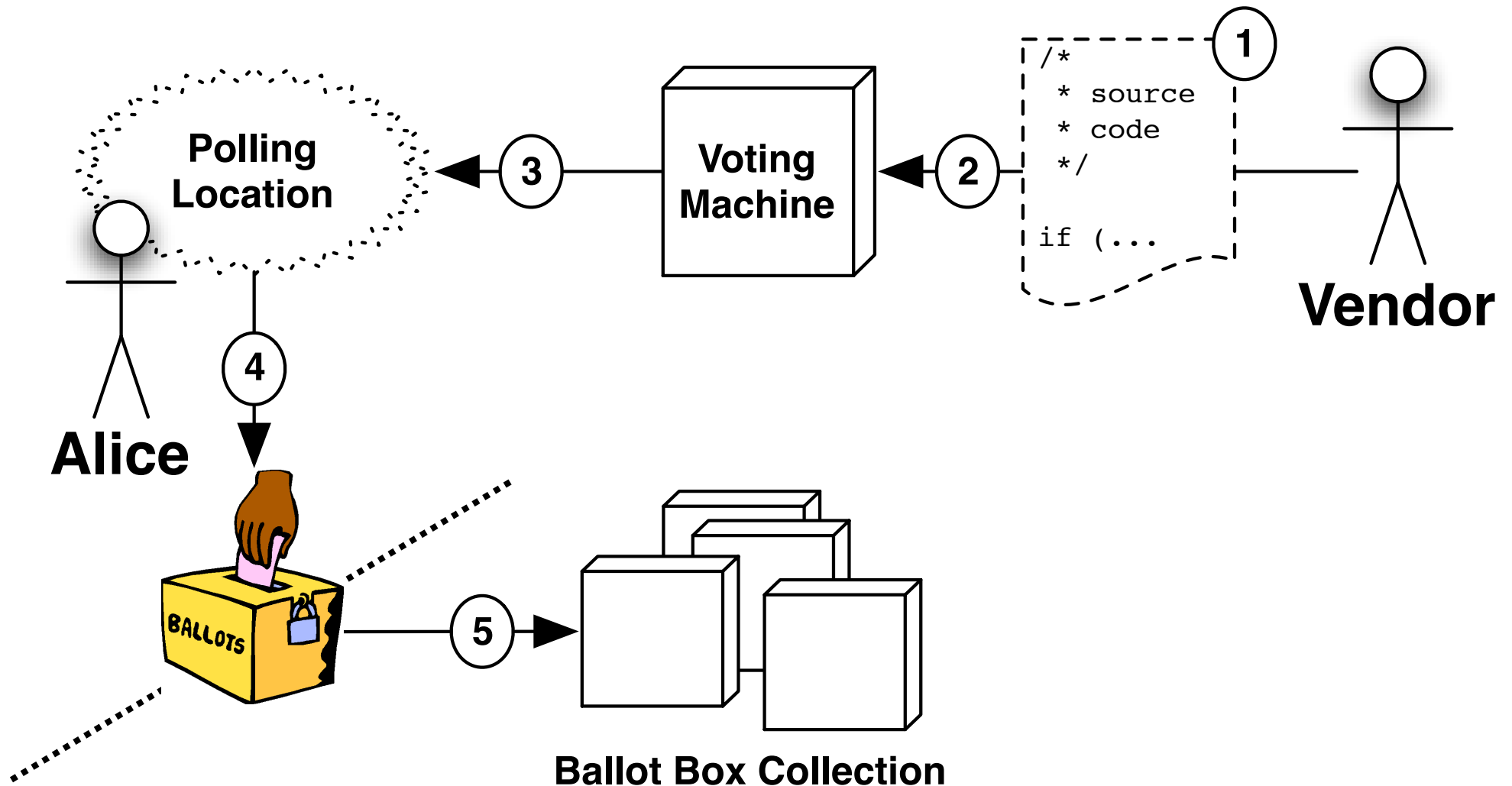
Chain of Custody



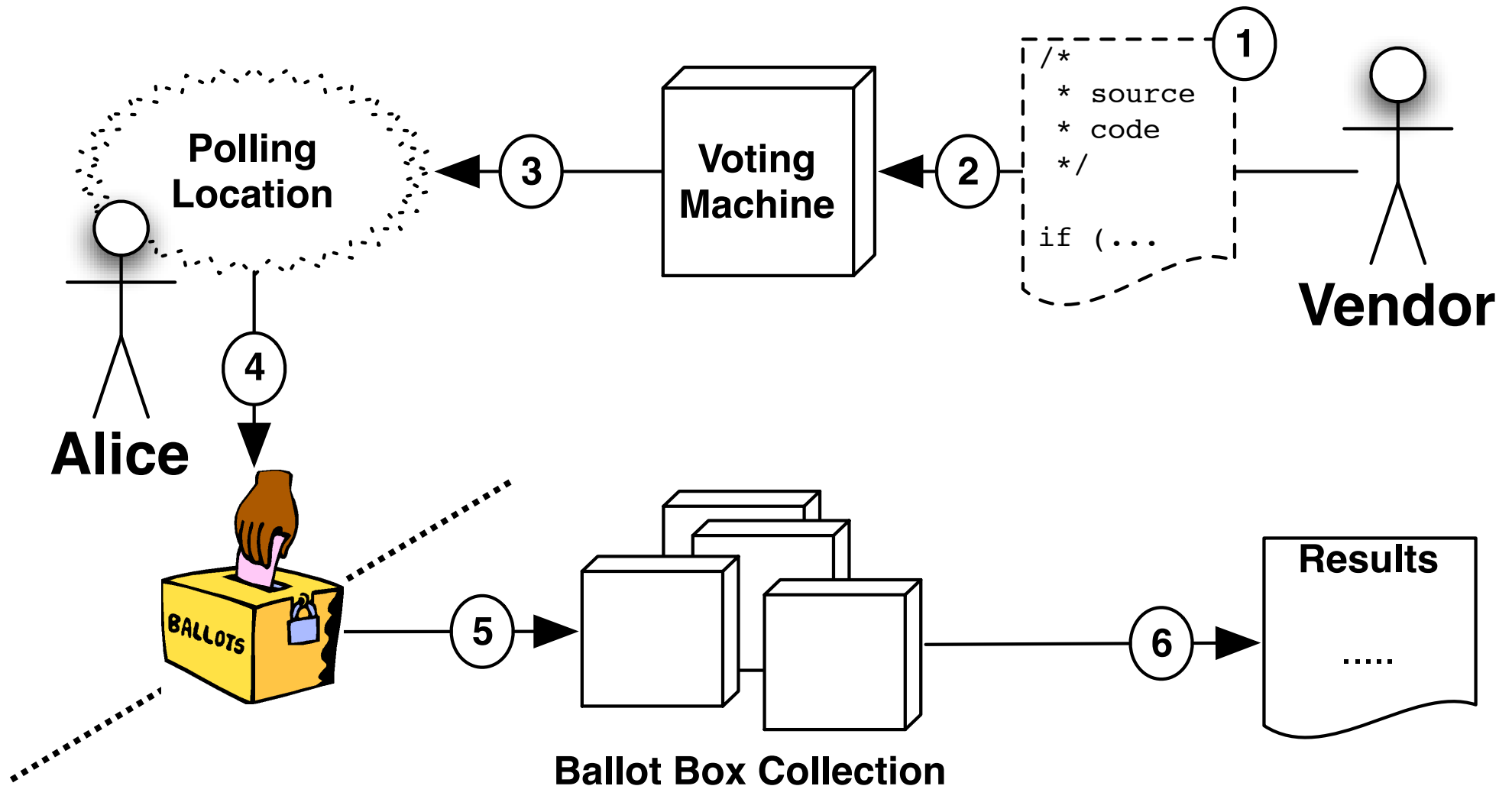
Chain of Custody



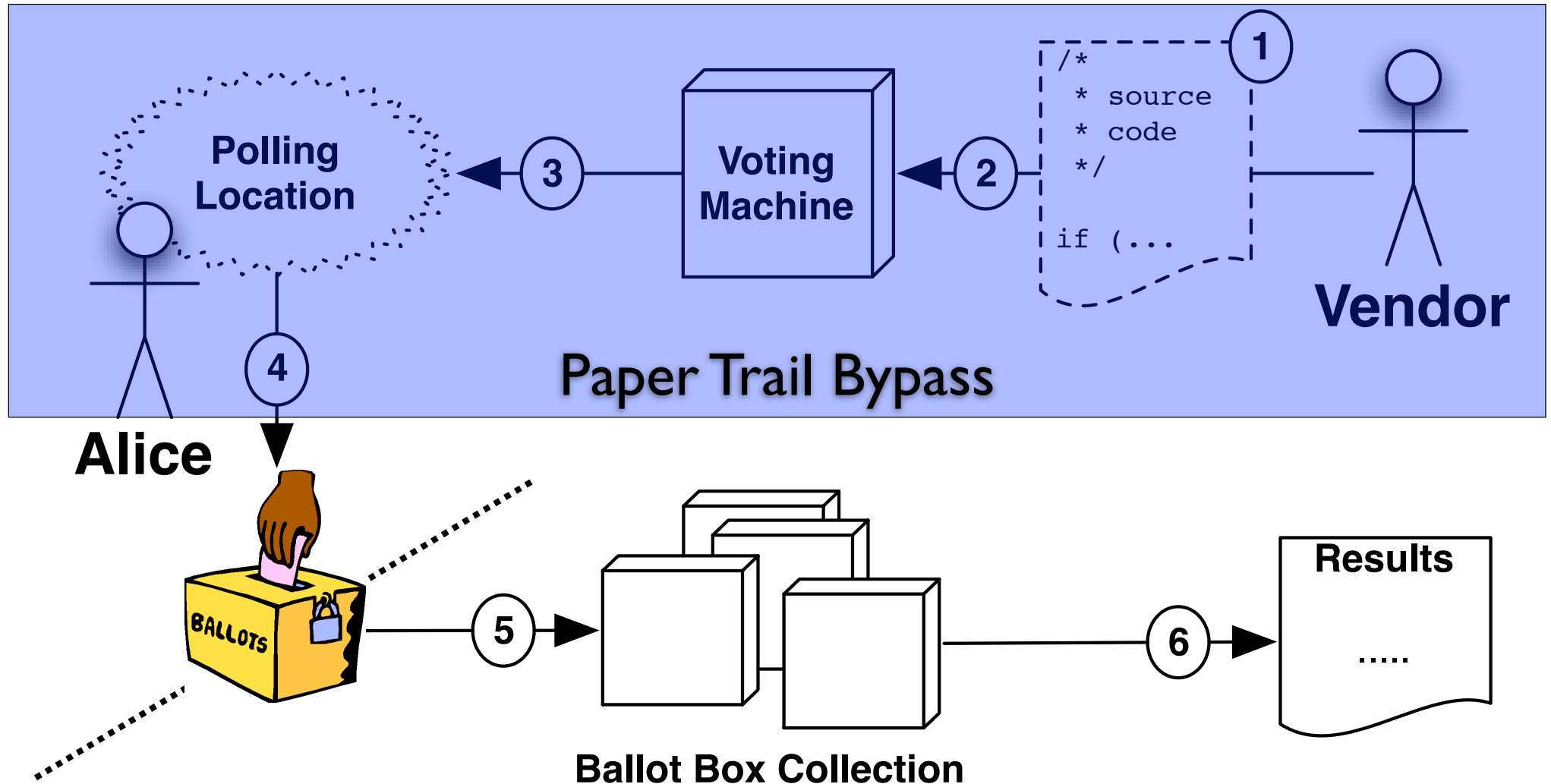
Chain of Custody



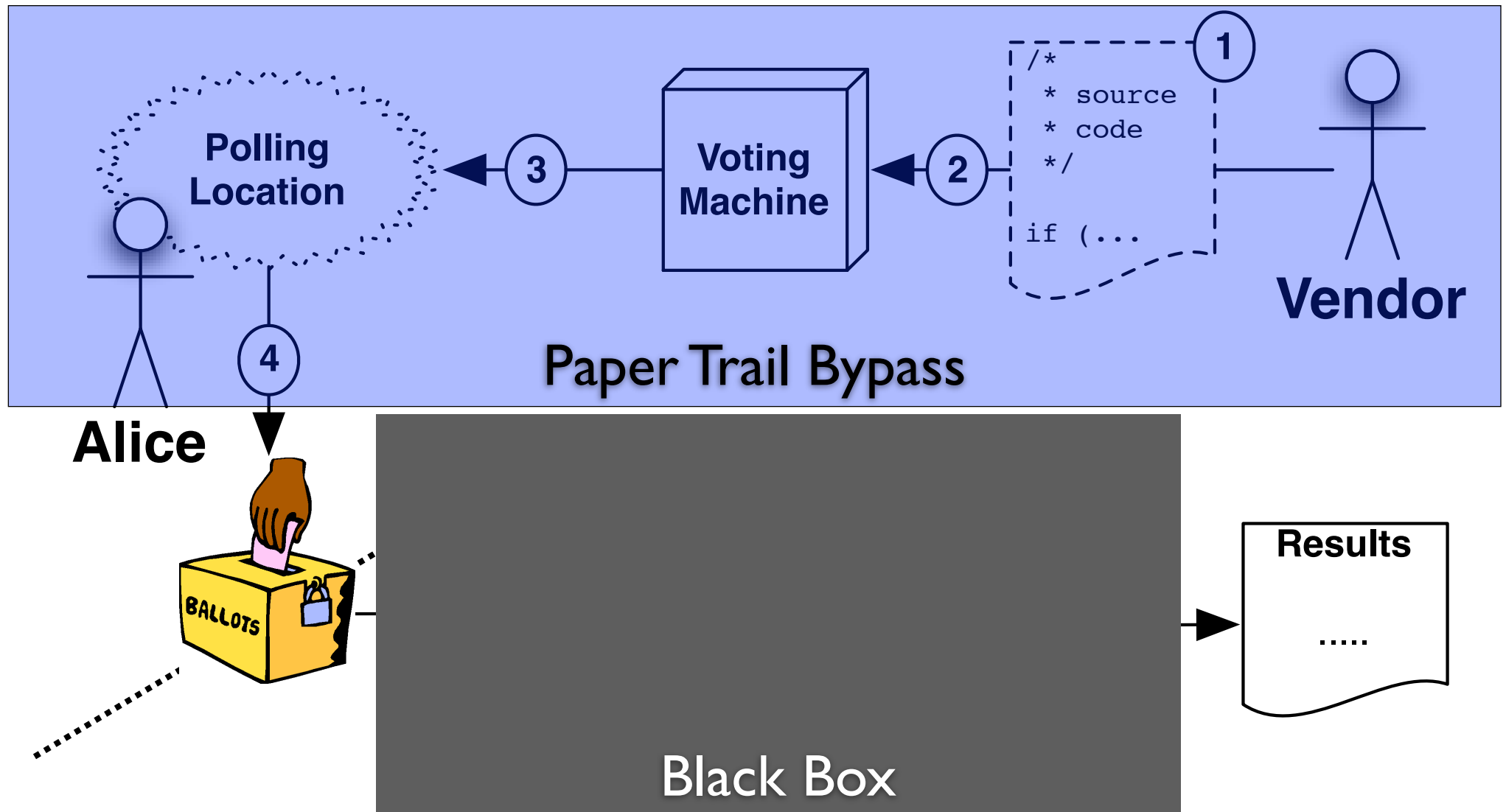
Chain of Custody



Chain of Custody



Chain of Custody



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, 1

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, 1

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, 1

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
election officials said.

**Mexico Presidential Election
Ballots Found in Dump**

RAW STORY

Published: Thursday July 6, 2006

The Cost of Secrecy

Scavenged **ballot box** lids haunt S.F. elections

[Erin McC](#)

Monday, 1

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 election officials said.

Mexico Presidential Election
Ballot Box in Dump

SARASOTA

18,000 votes in U.S. House race may be lost

Thousands of votes were either not counted or not cast in Sarasota's nationally watched congressional race.

Is Secrecy Important?

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]

Open-Audit Voting

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

Properties of OAV

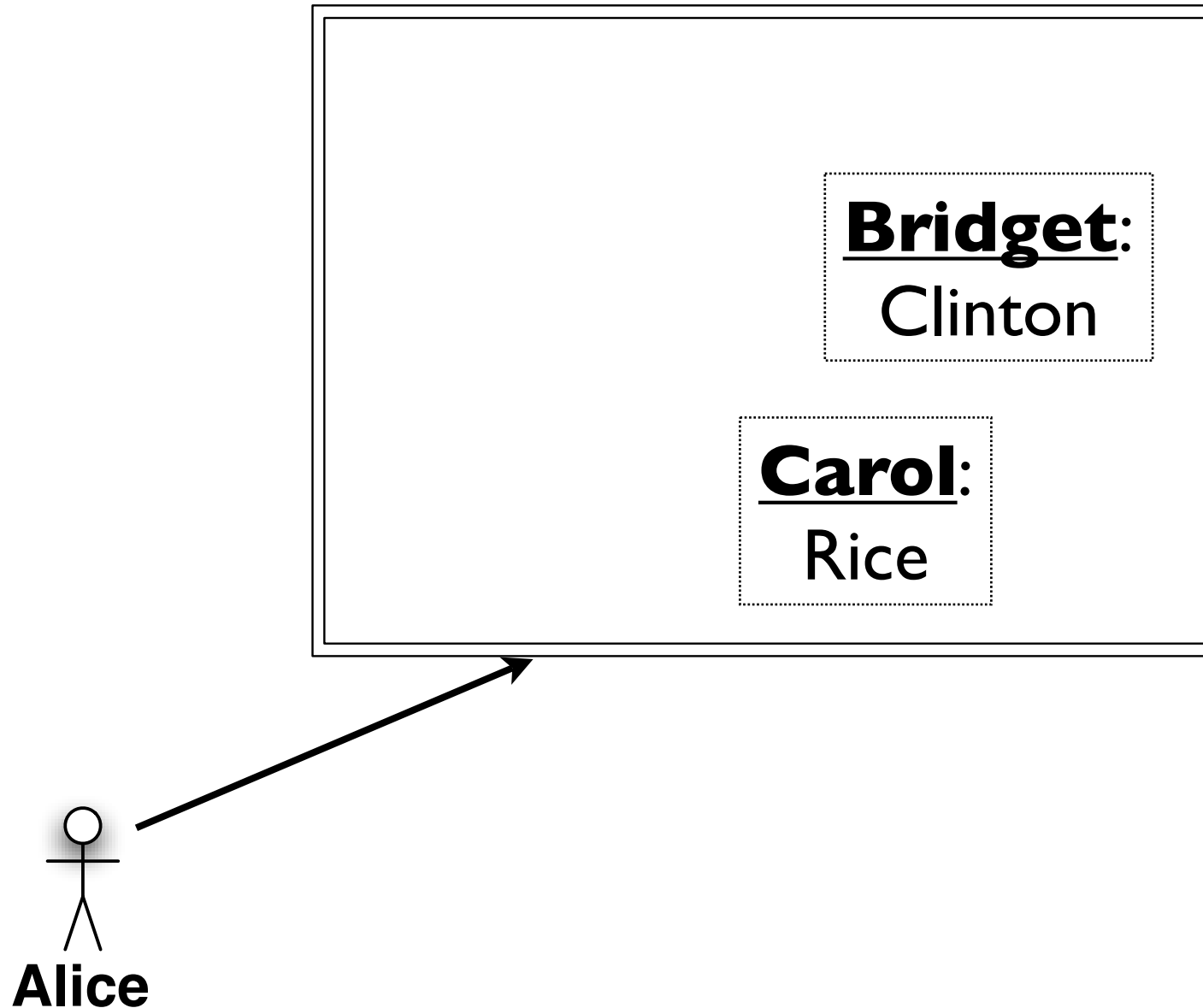
- (1) **Alice** verifies **her vote**.
- (2) **Everyone** verifies **tallying**.
- (3) Alice **cannot be coerced** by Eve.

Public Ballots

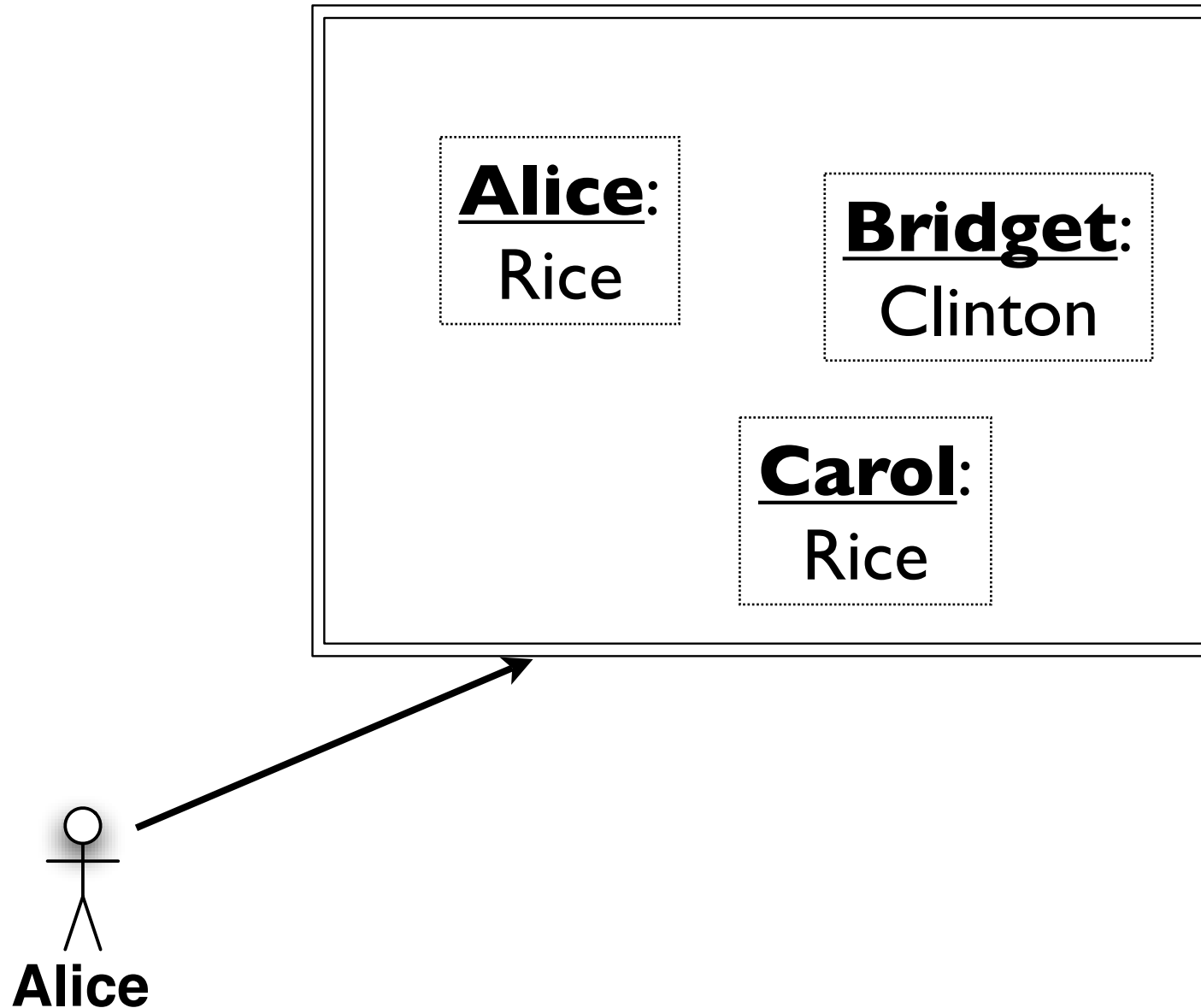
Bridget:
Clinton

Carol:
Rice

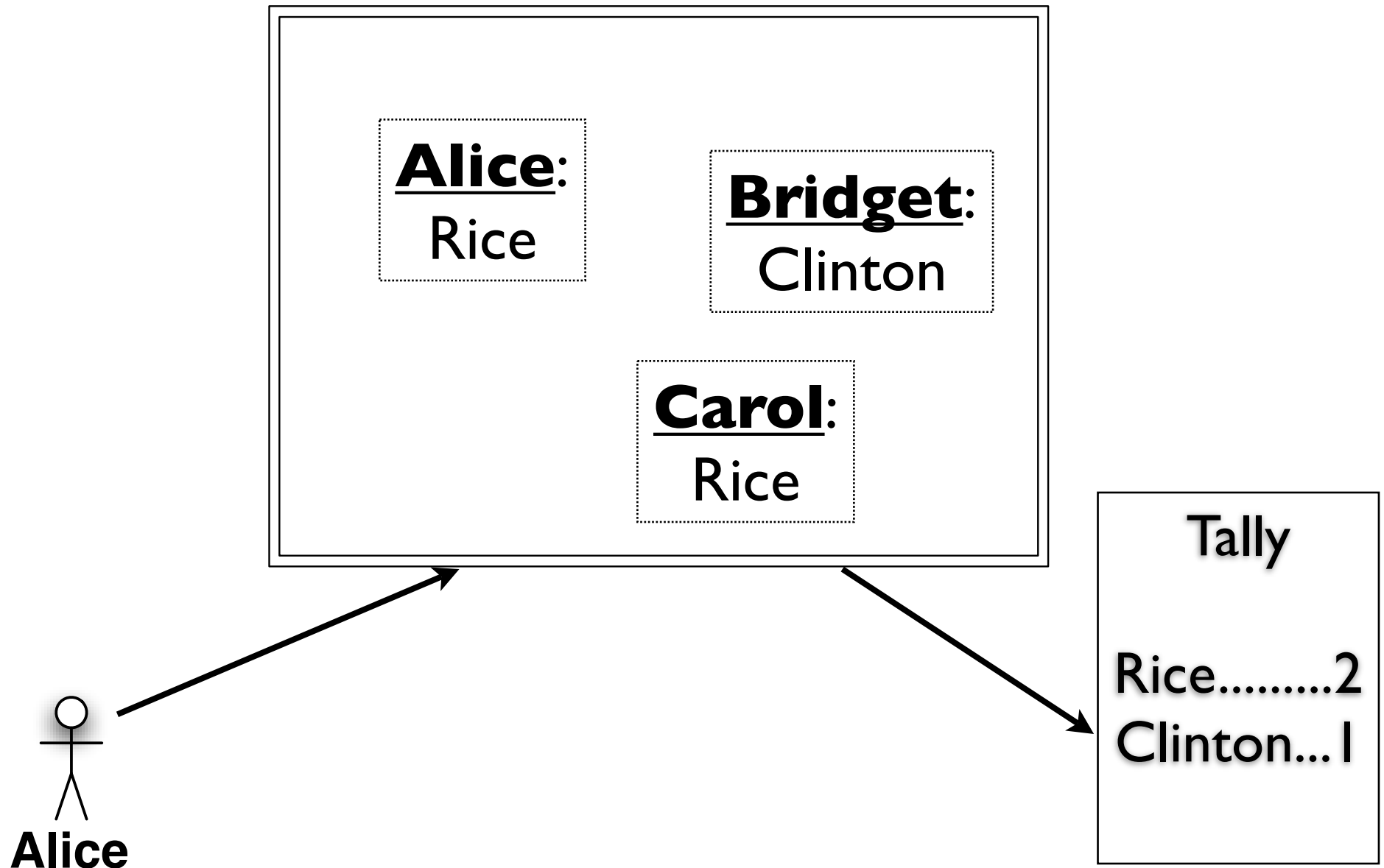
Public Ballots



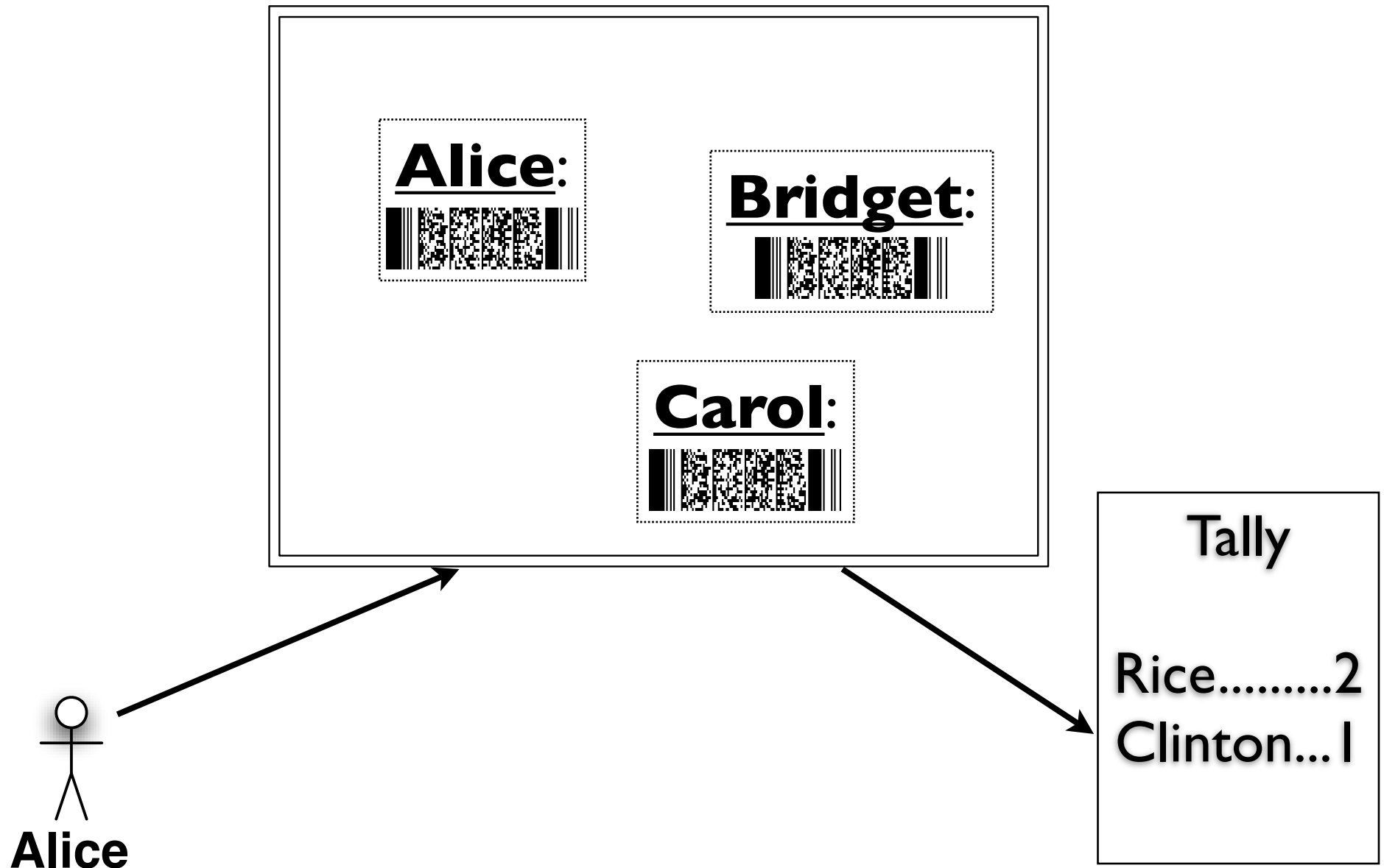
Public Ballots



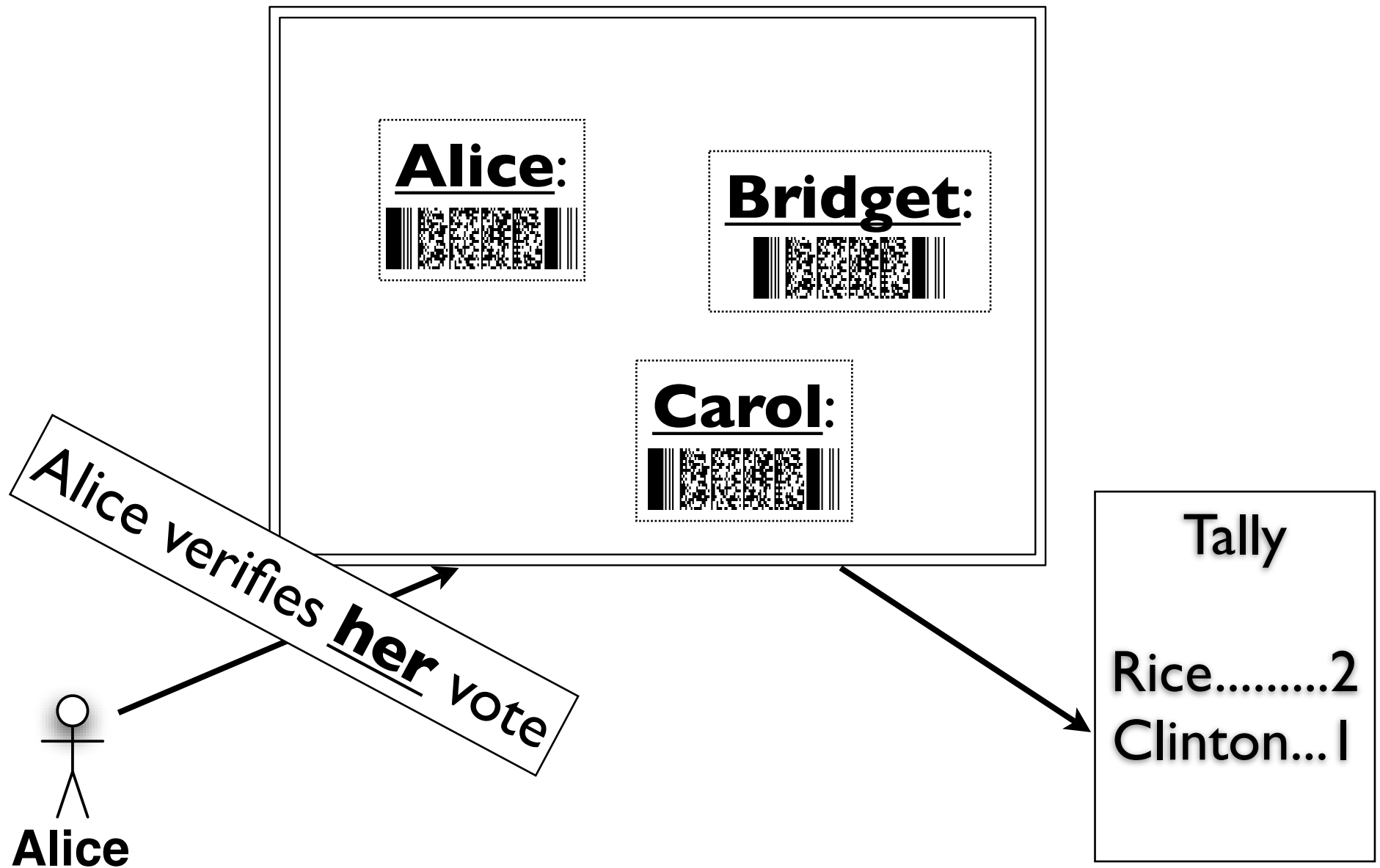
Public Ballots



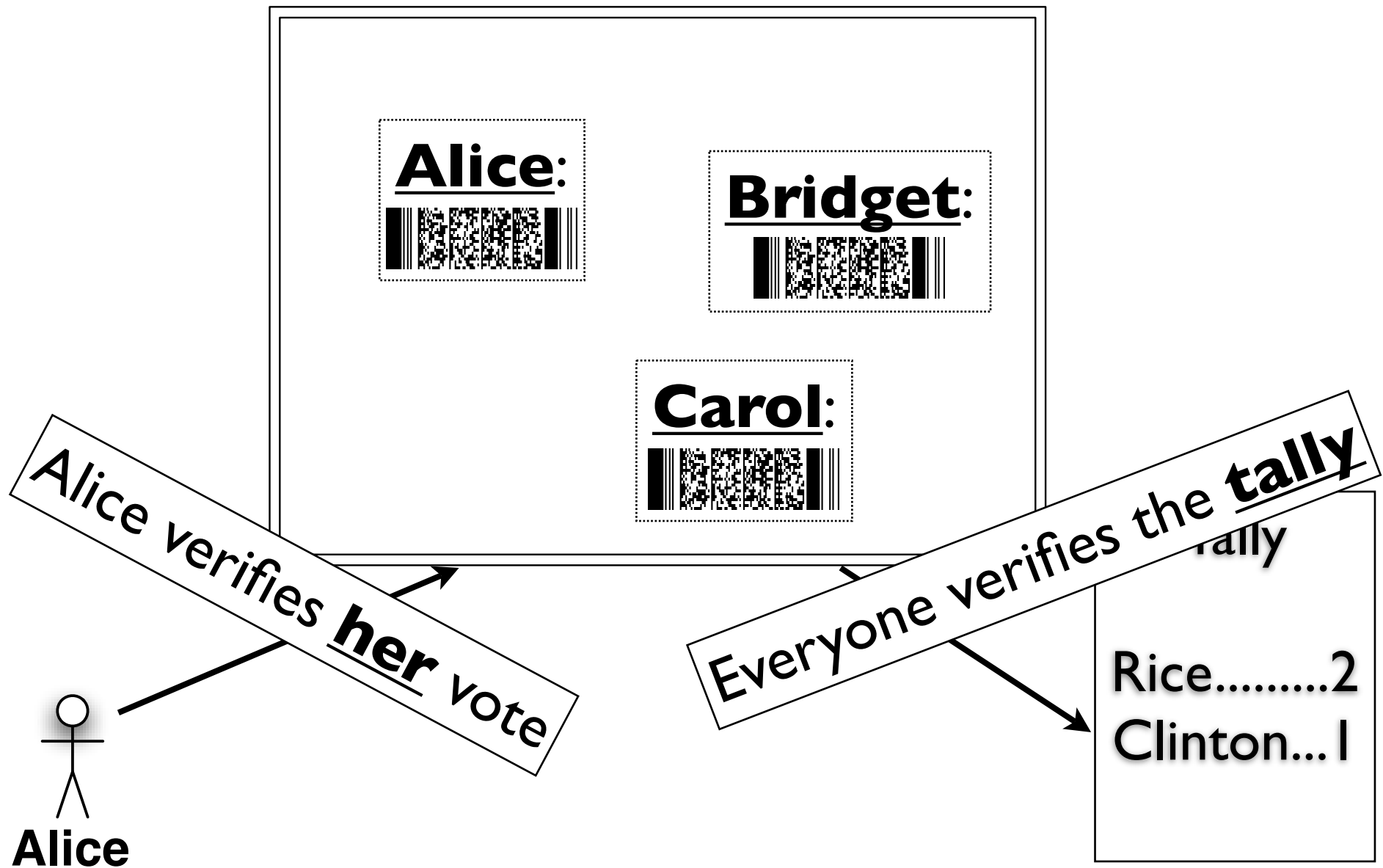
Encrypted Public Ballots

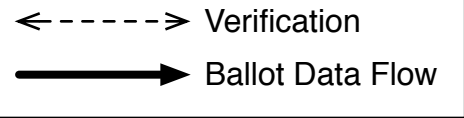


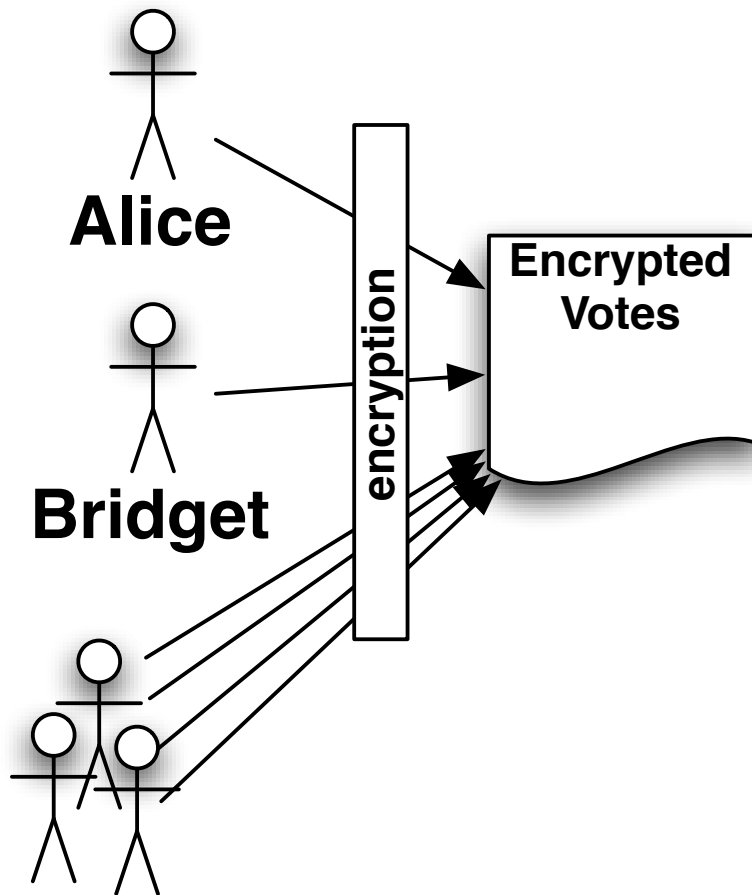
Encrypted Public Ballots



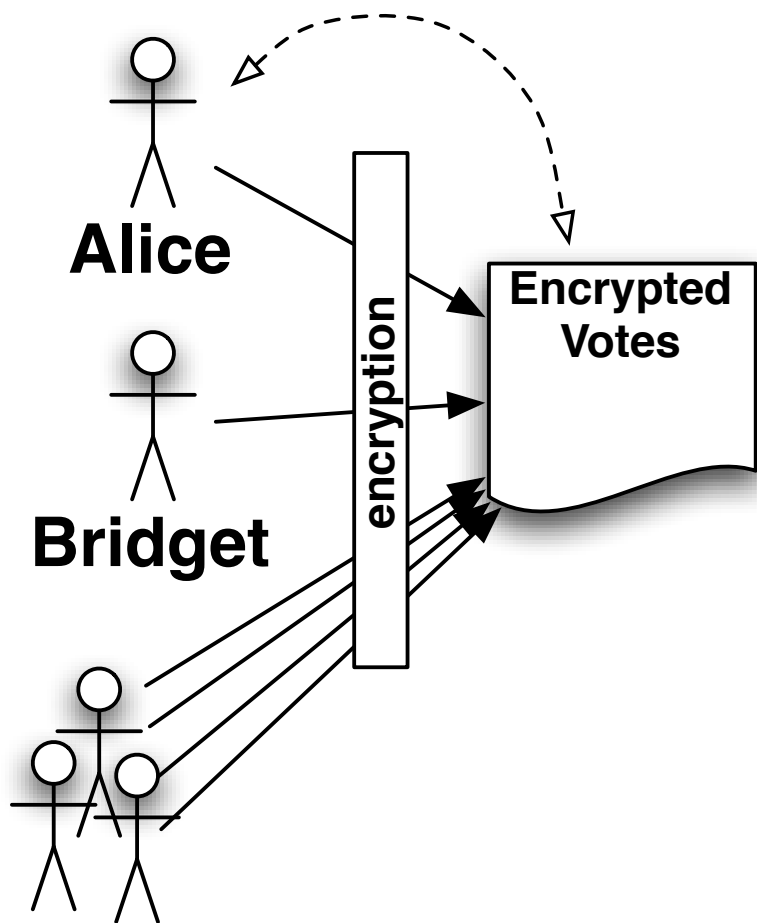
Encrypted Public Ballots



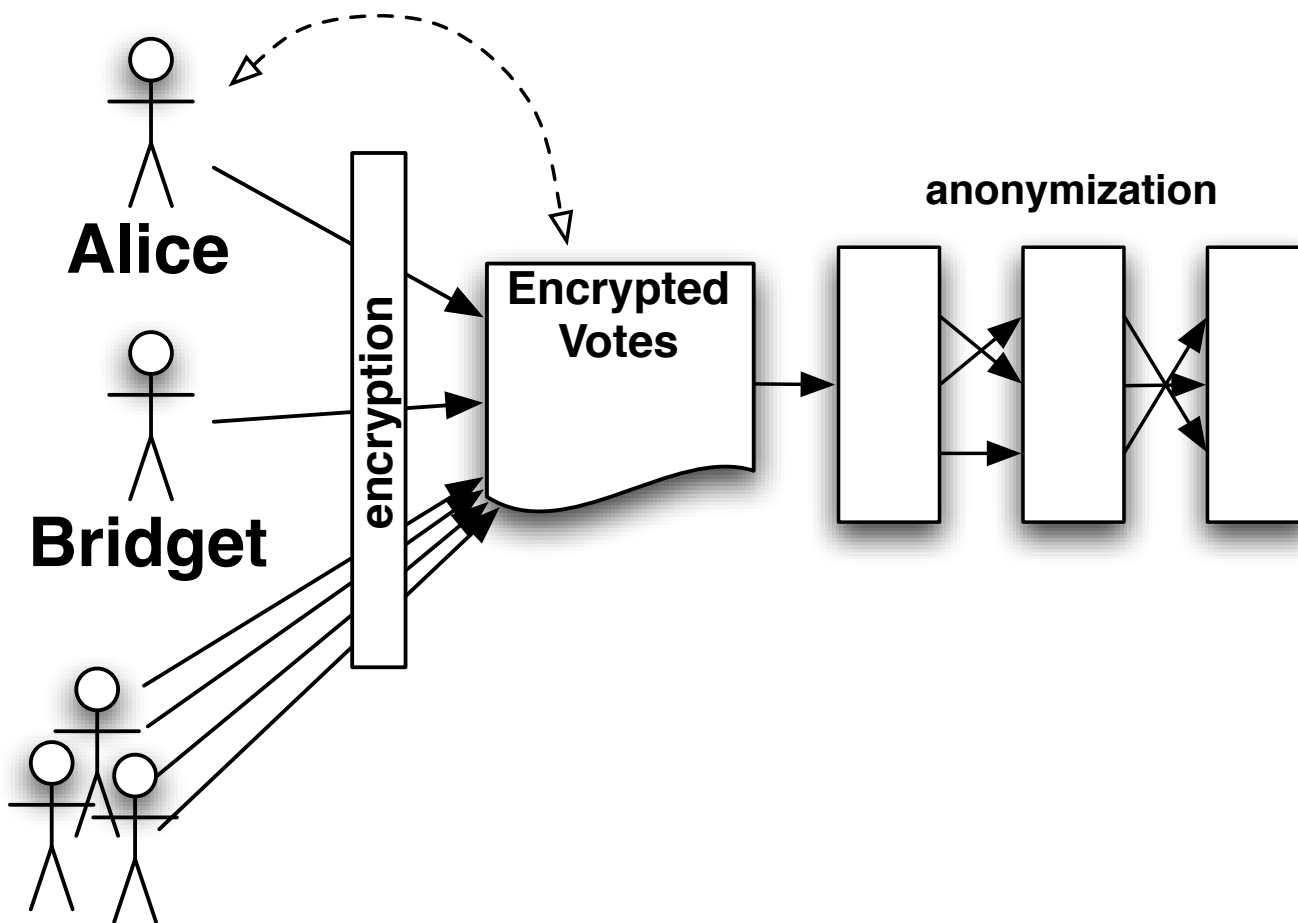




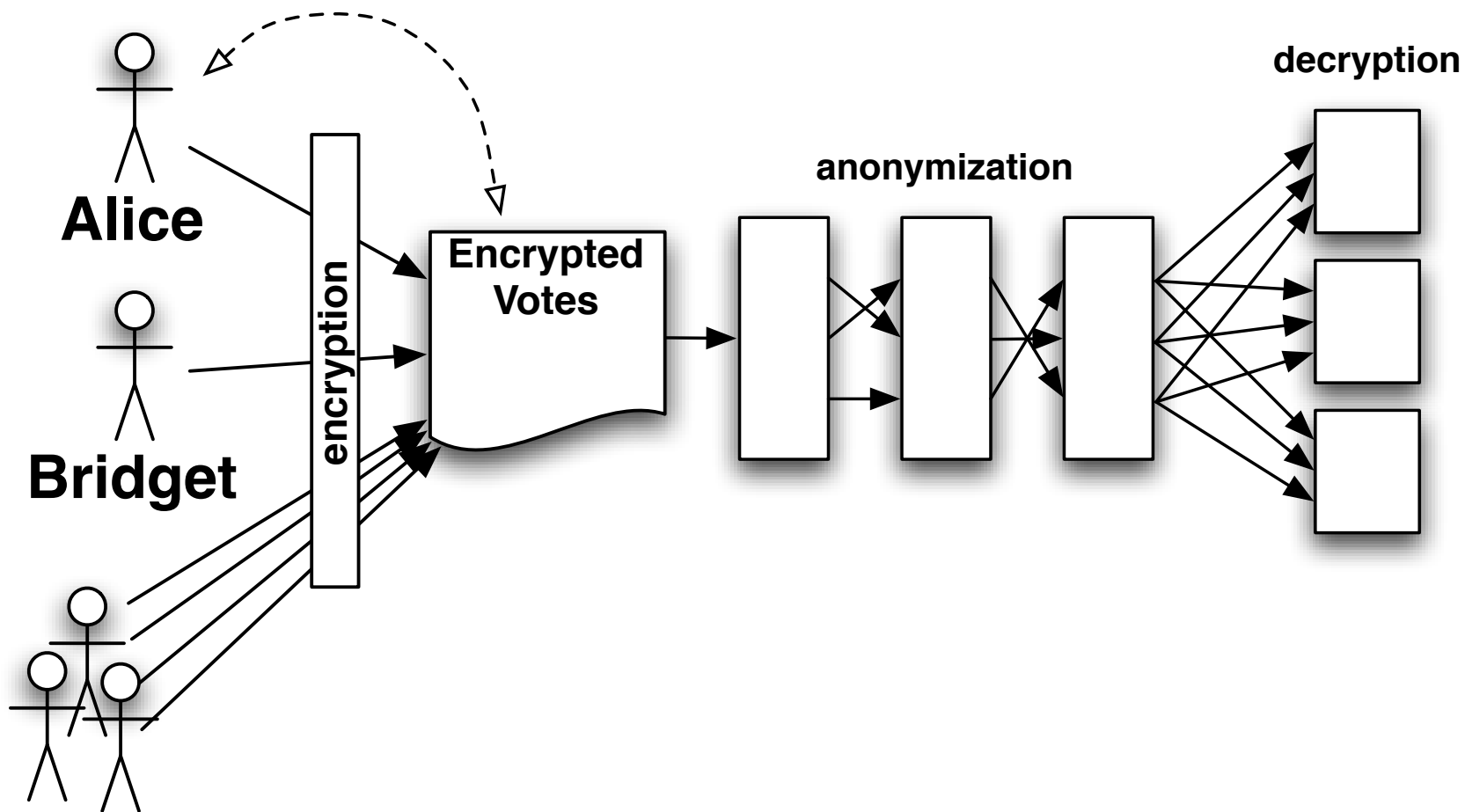
←-----> Verification
—————> Ballot Data Flow



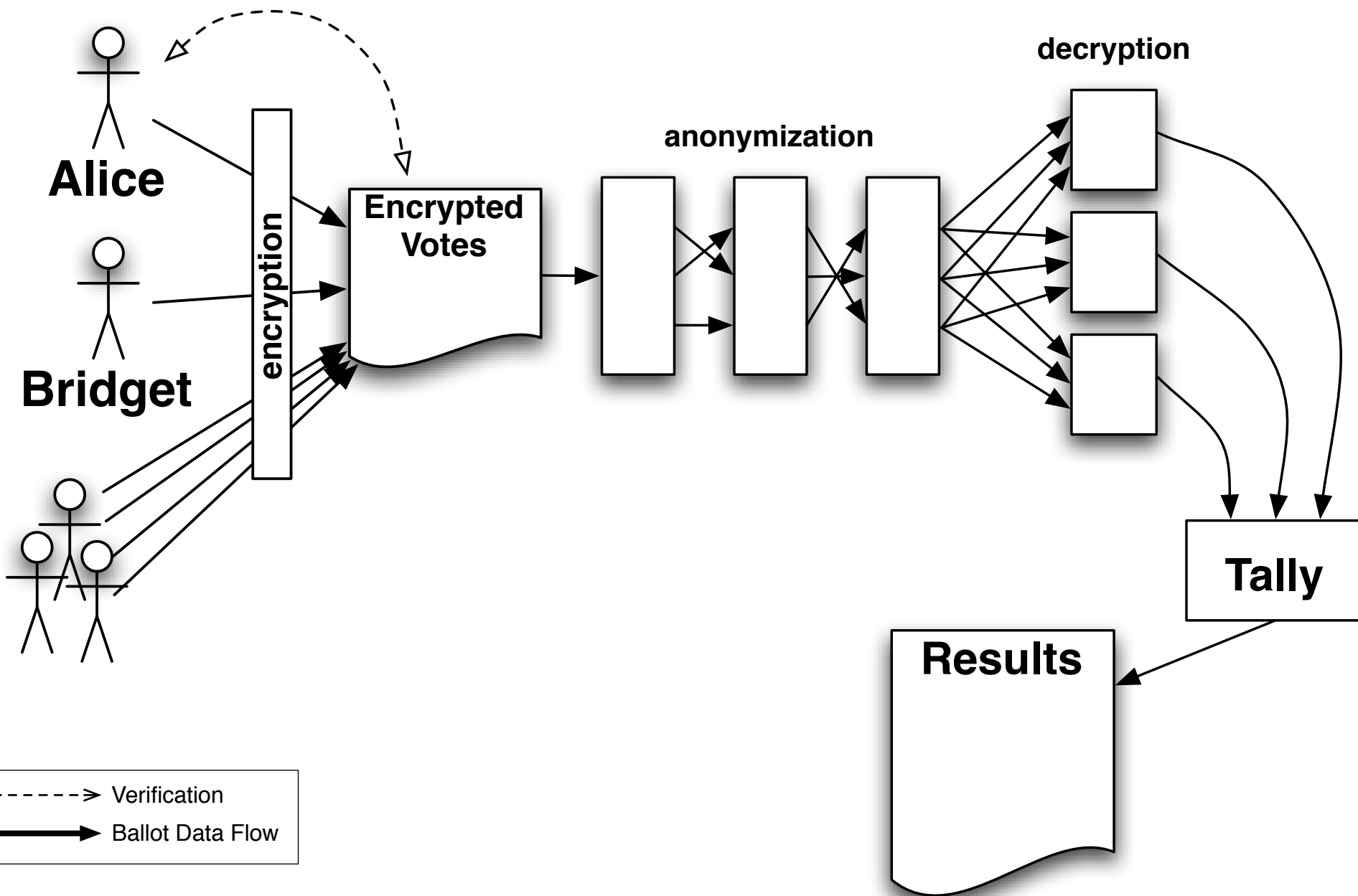
←-----> Verification
—————> Ballot Data Flow

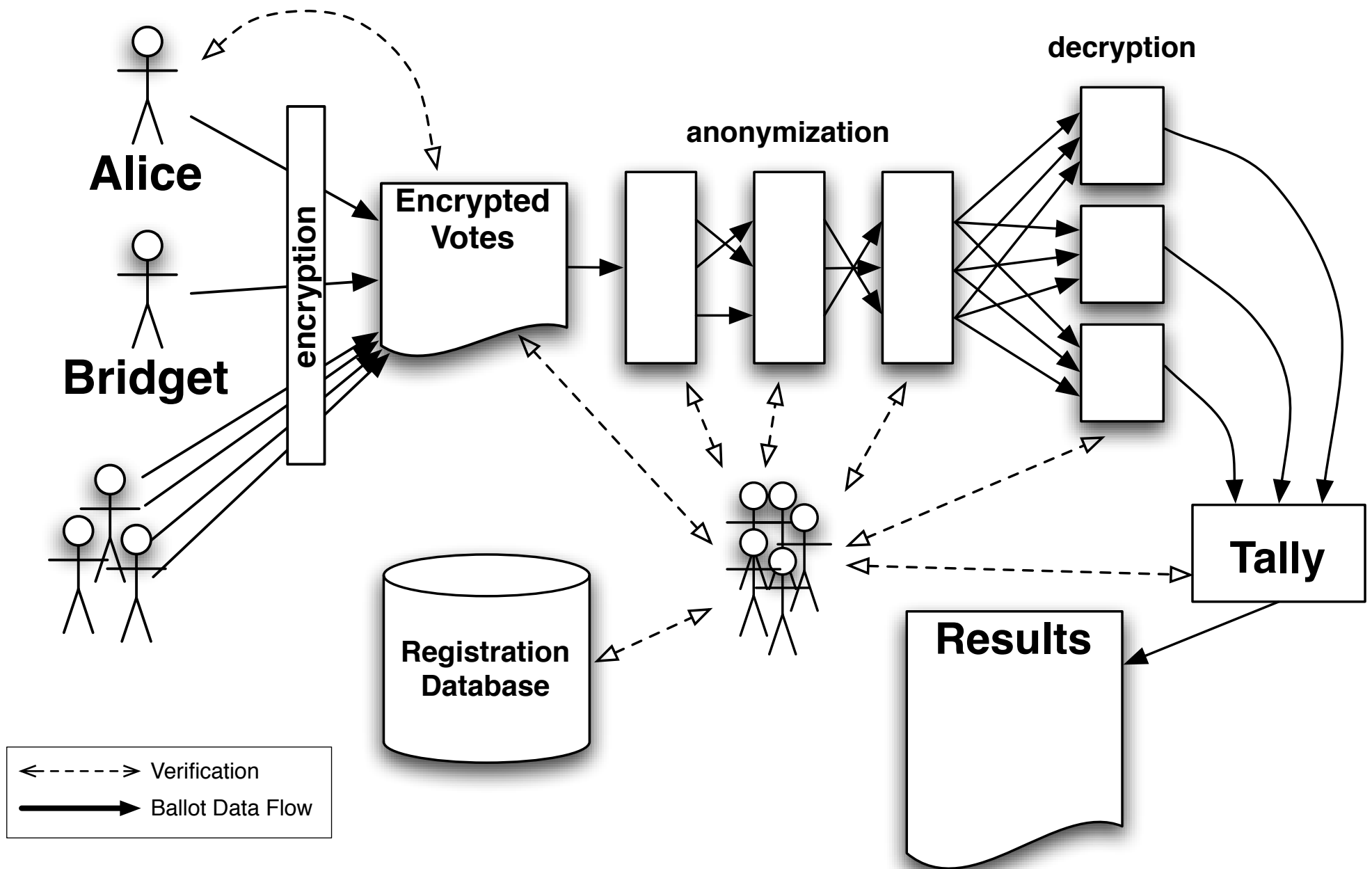


←-----> Verification
—————> Ballot Data Flow



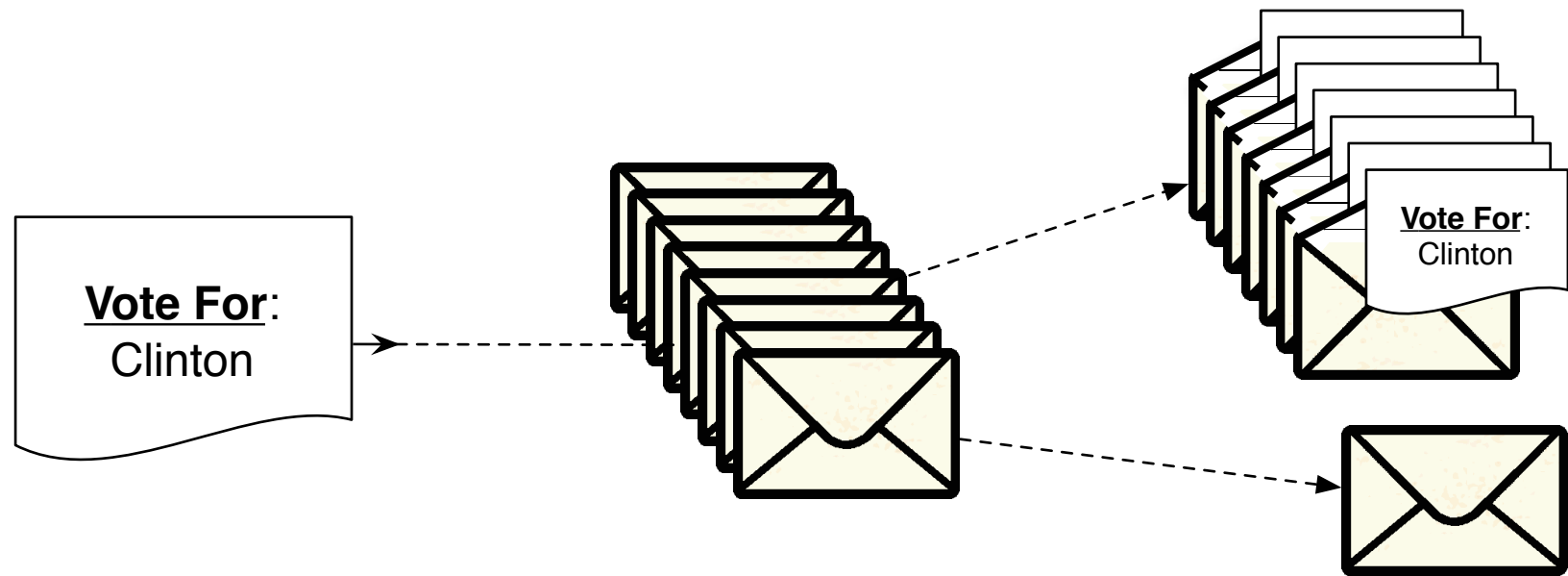
←-----> Verification
—————> Ballot Data Flow



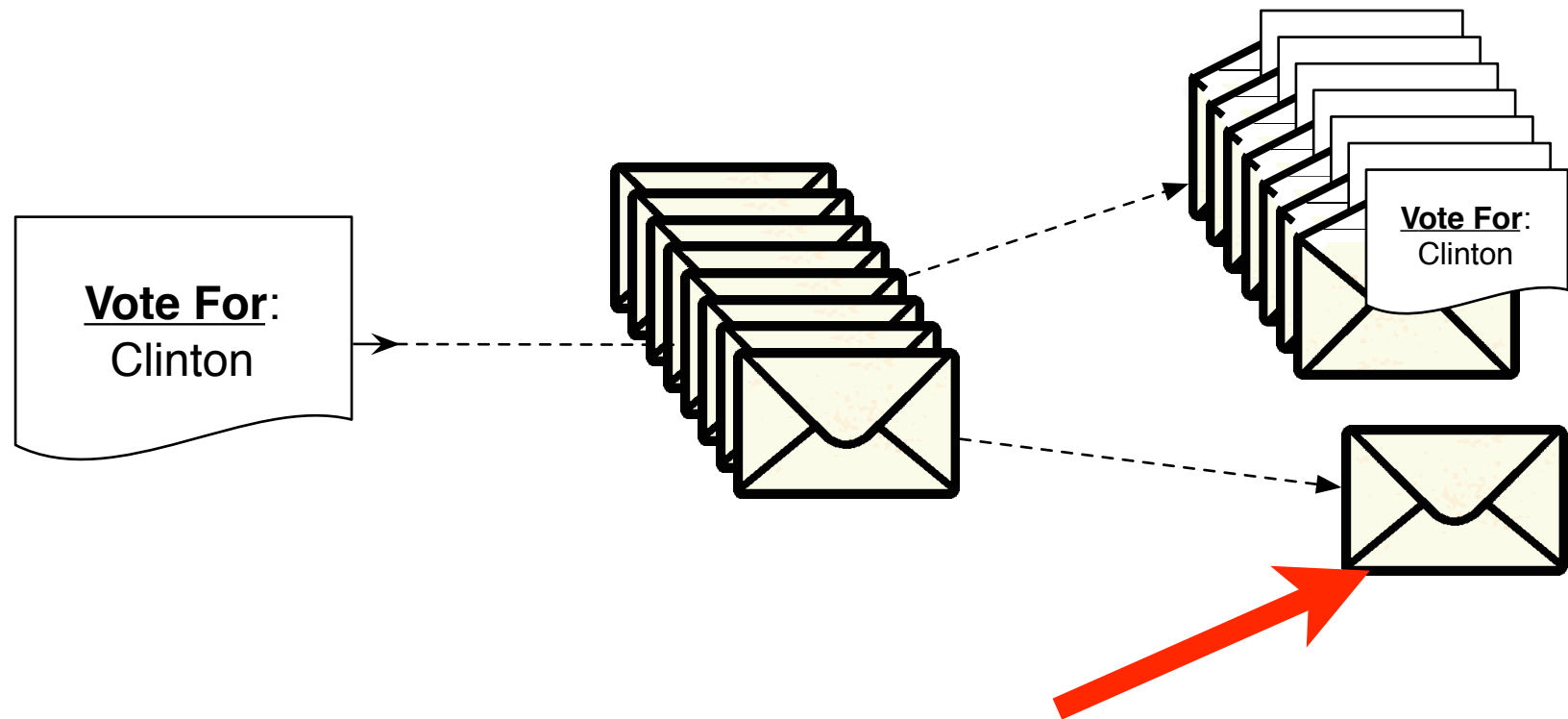


Zero-Knowledge Proof

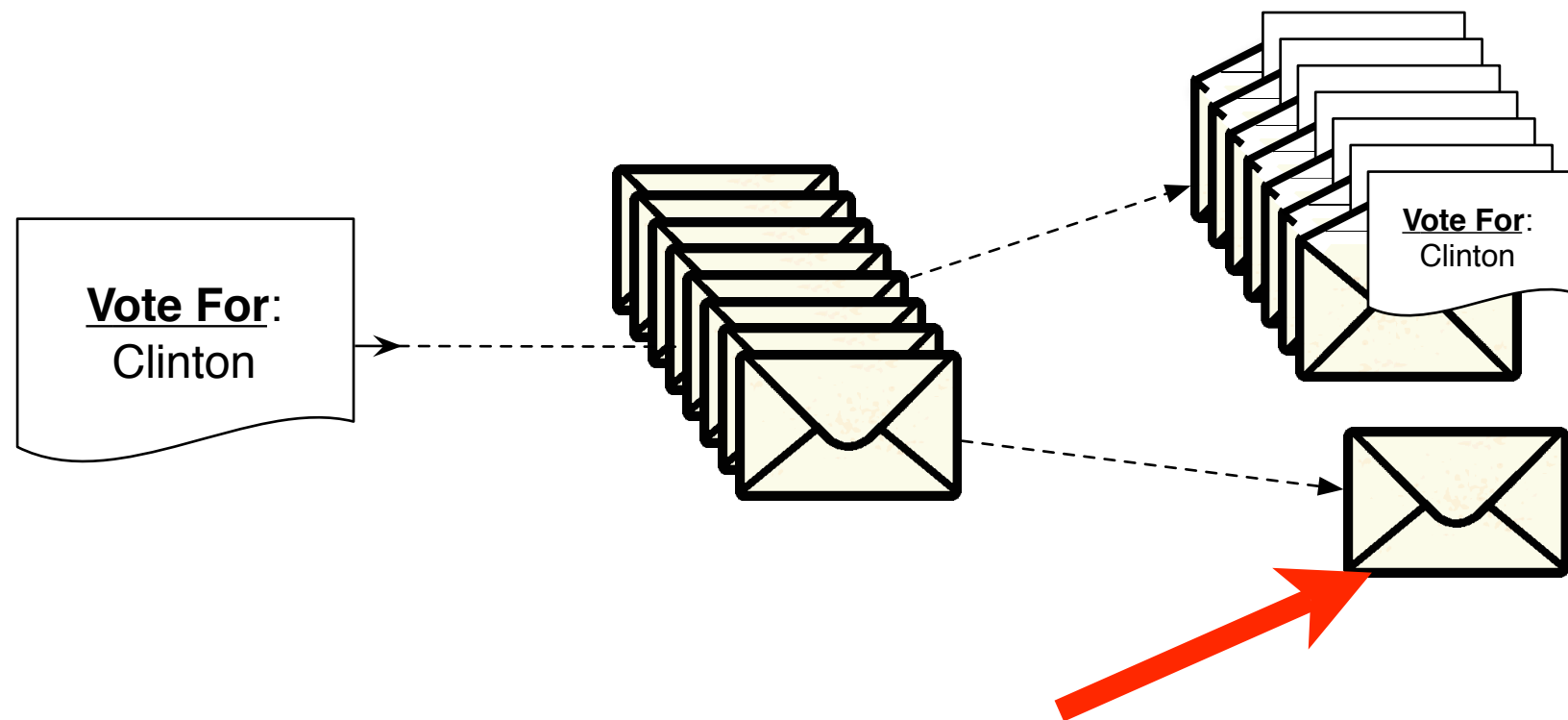
Zero-Knowledge Proof



Zero-Knowledge Proof

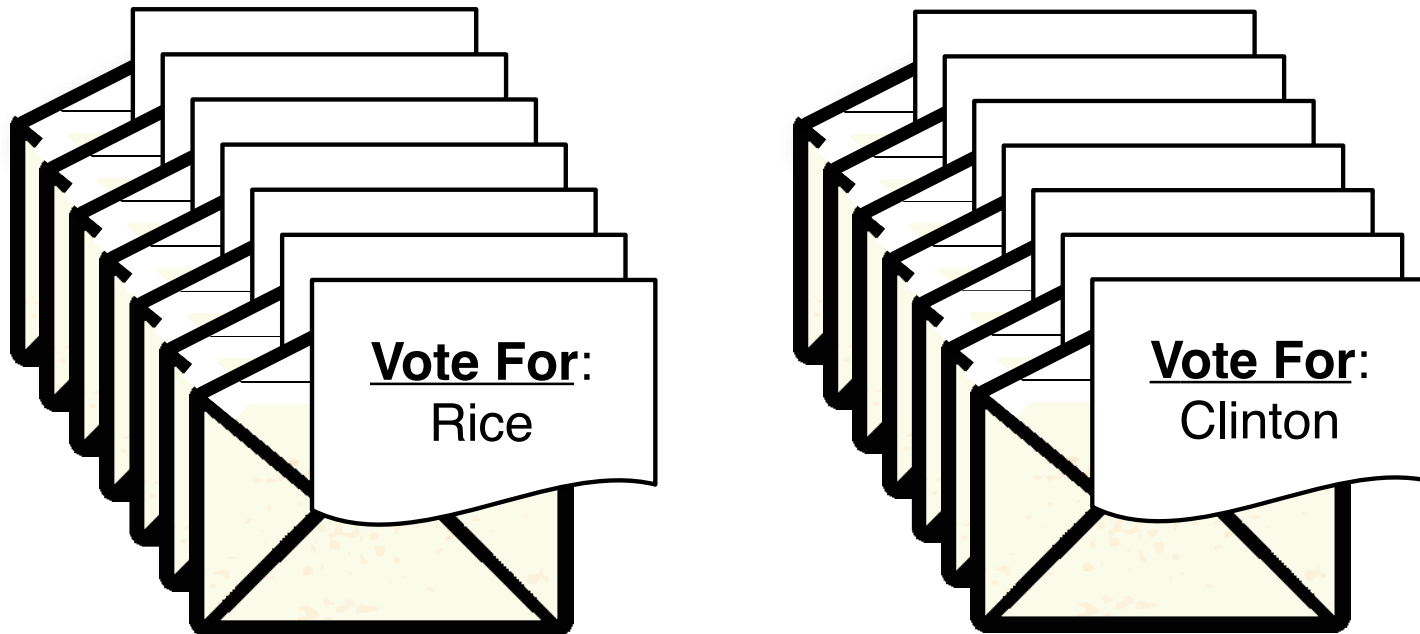


Zero-Knowledge Proof



This last envelope
likely contains "Clinton"

Zero-Knowledge Proof



Open envelopes don't prove
anything after the fact.

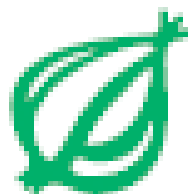
Scratch-and-Vote

Scratch-and-Vote

Scratch 'N Win Ballots To Debut In November

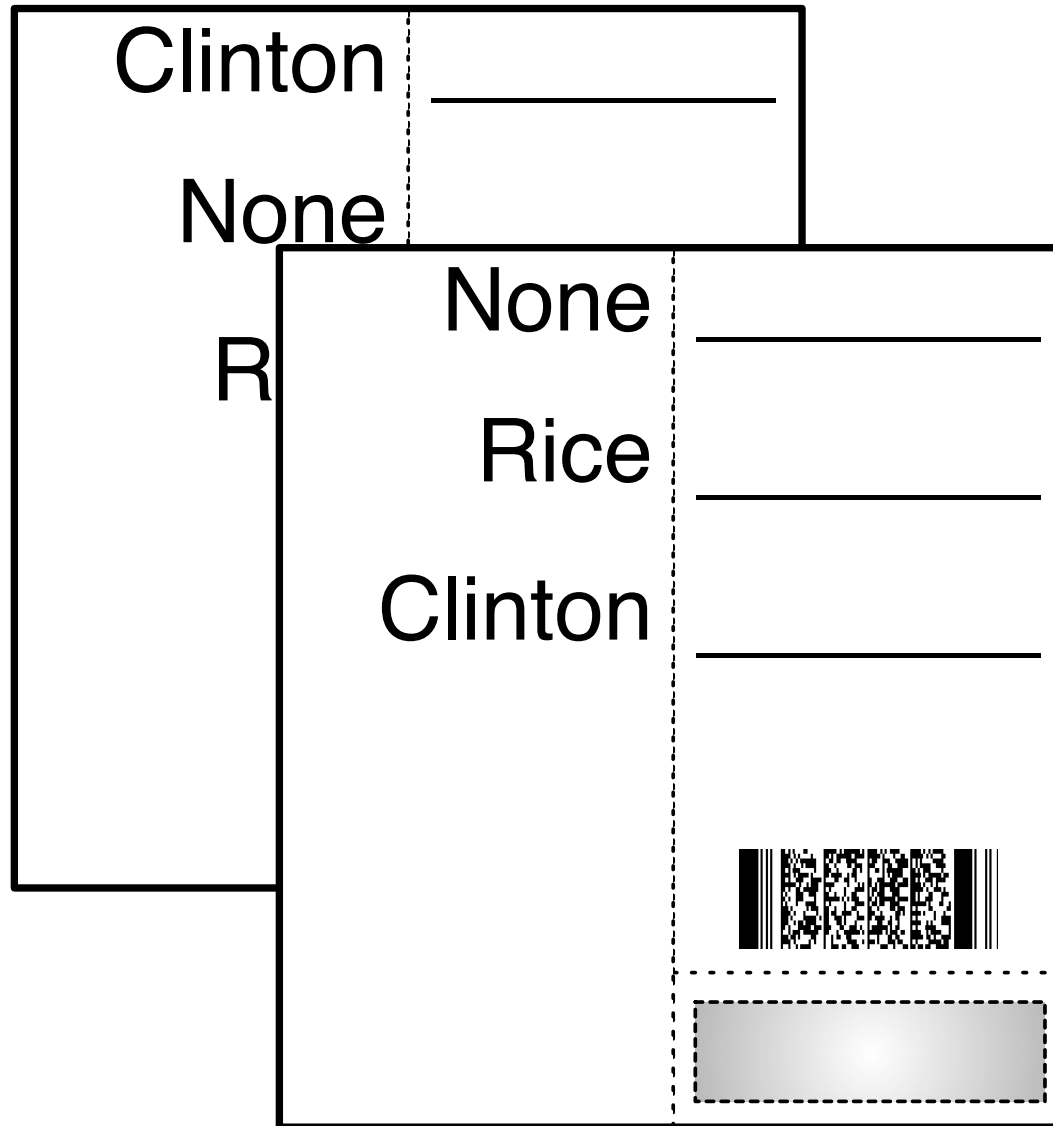
July 19, 2006 | Issue 42•29

WASHINGTON, DC—In an effort to increase voter participation while generating additional revenue, several state election boards announced plans Monday to introduce new Scratch 'N Win ballots in November, giving citizens the chance to win the right to vote in the 2006 elections.

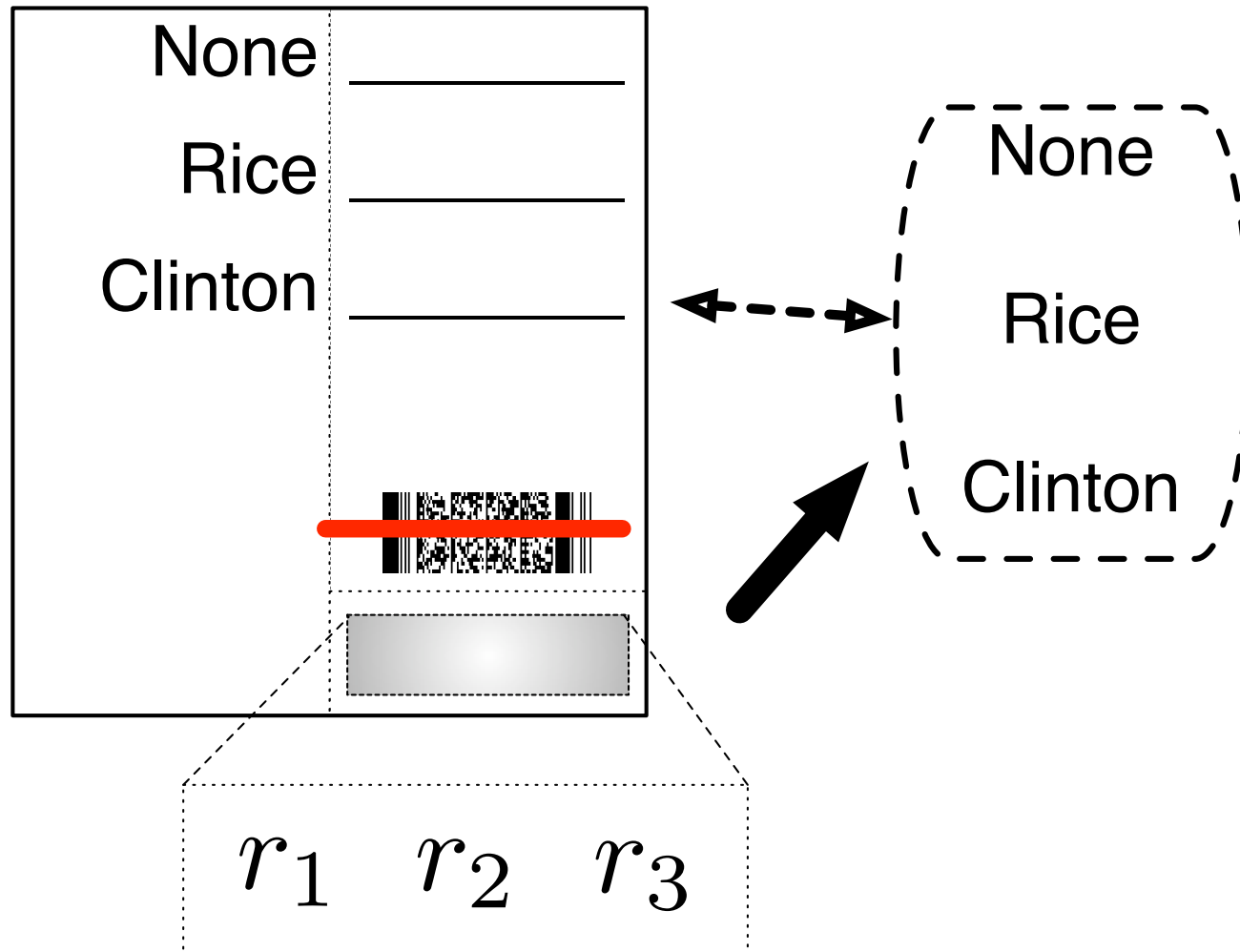


the ONION

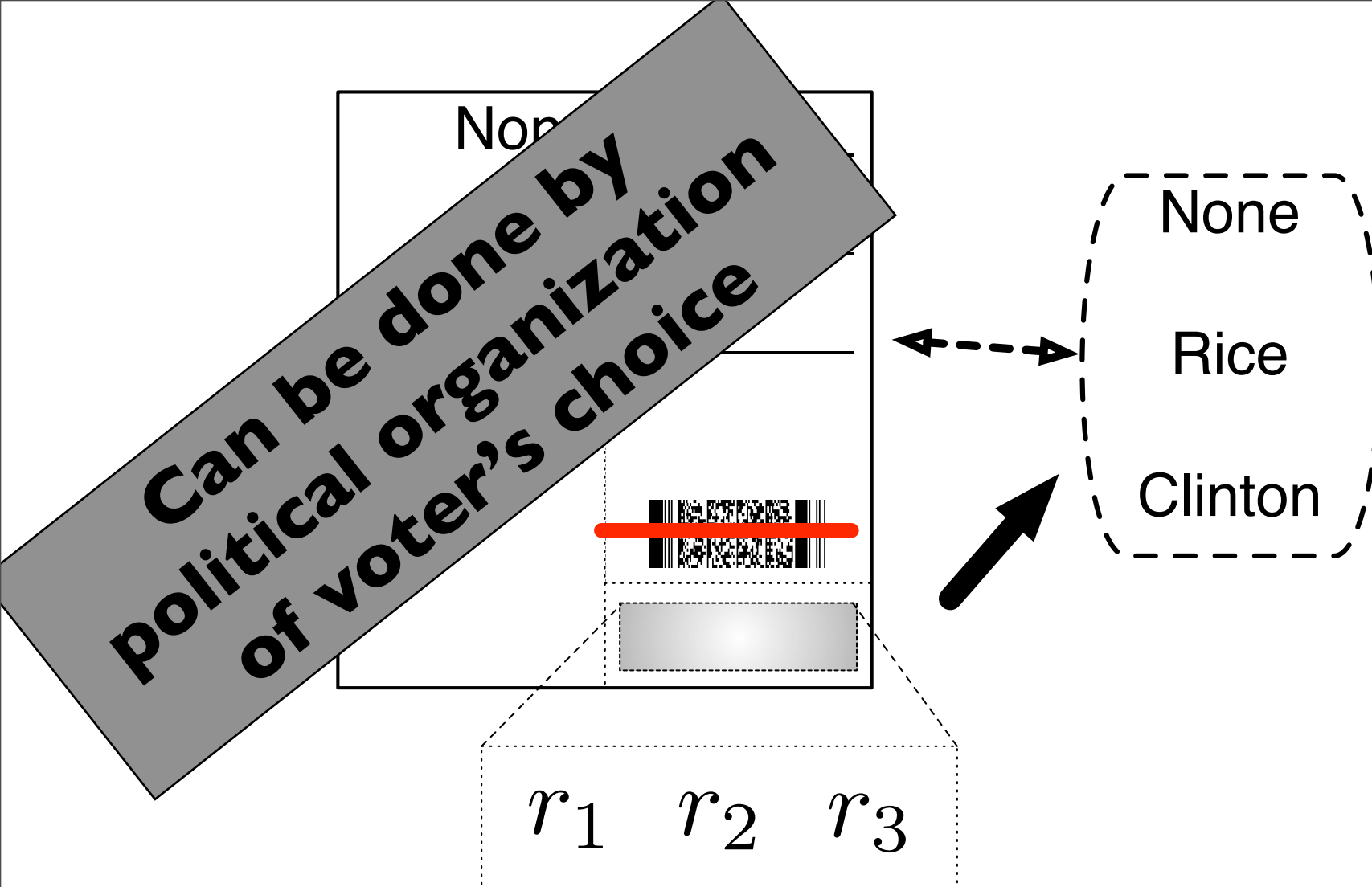
America's Finest News Source



1. Receive two ballots.






2. Choose one randomly
for auditing by scratch-off.



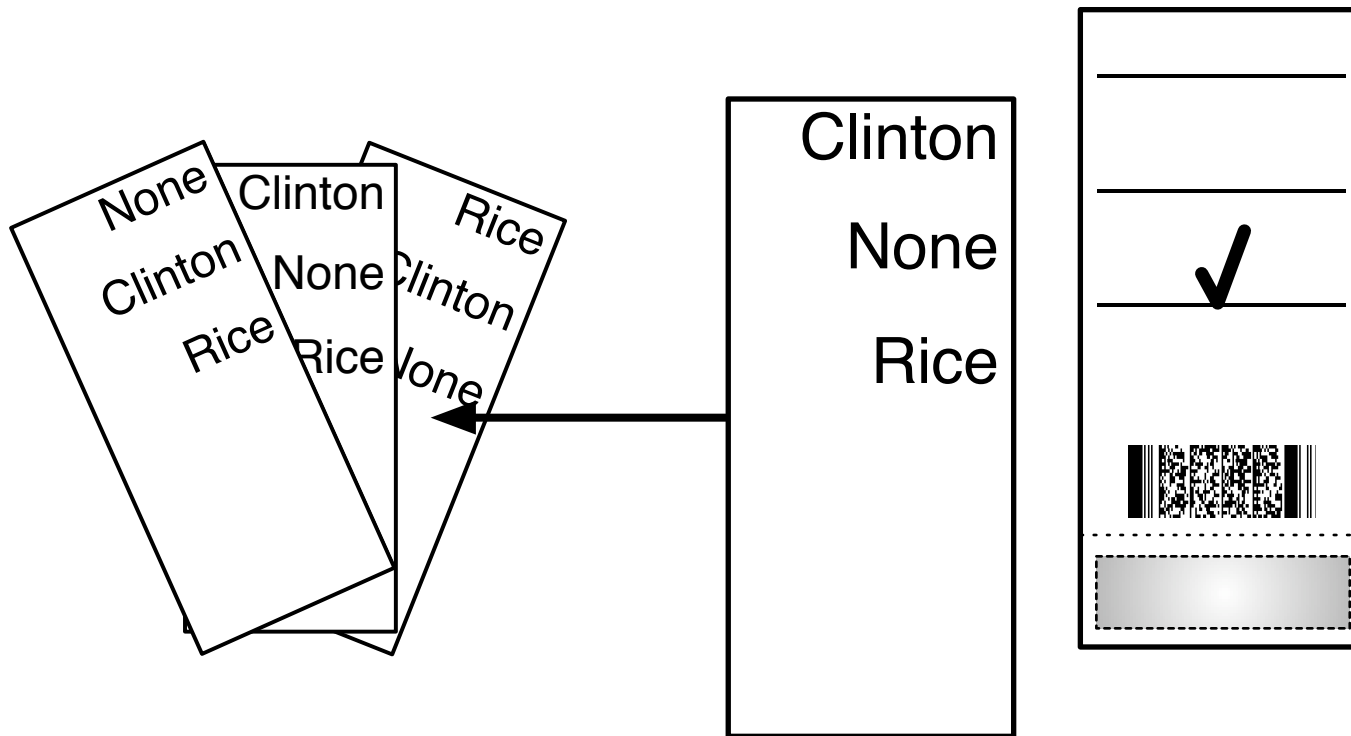
2. Choose one randomly for auditing by scratch-off.

In Private

Clinton	<hr/>
None	<hr/>
Rice	<hr/> 
	
	

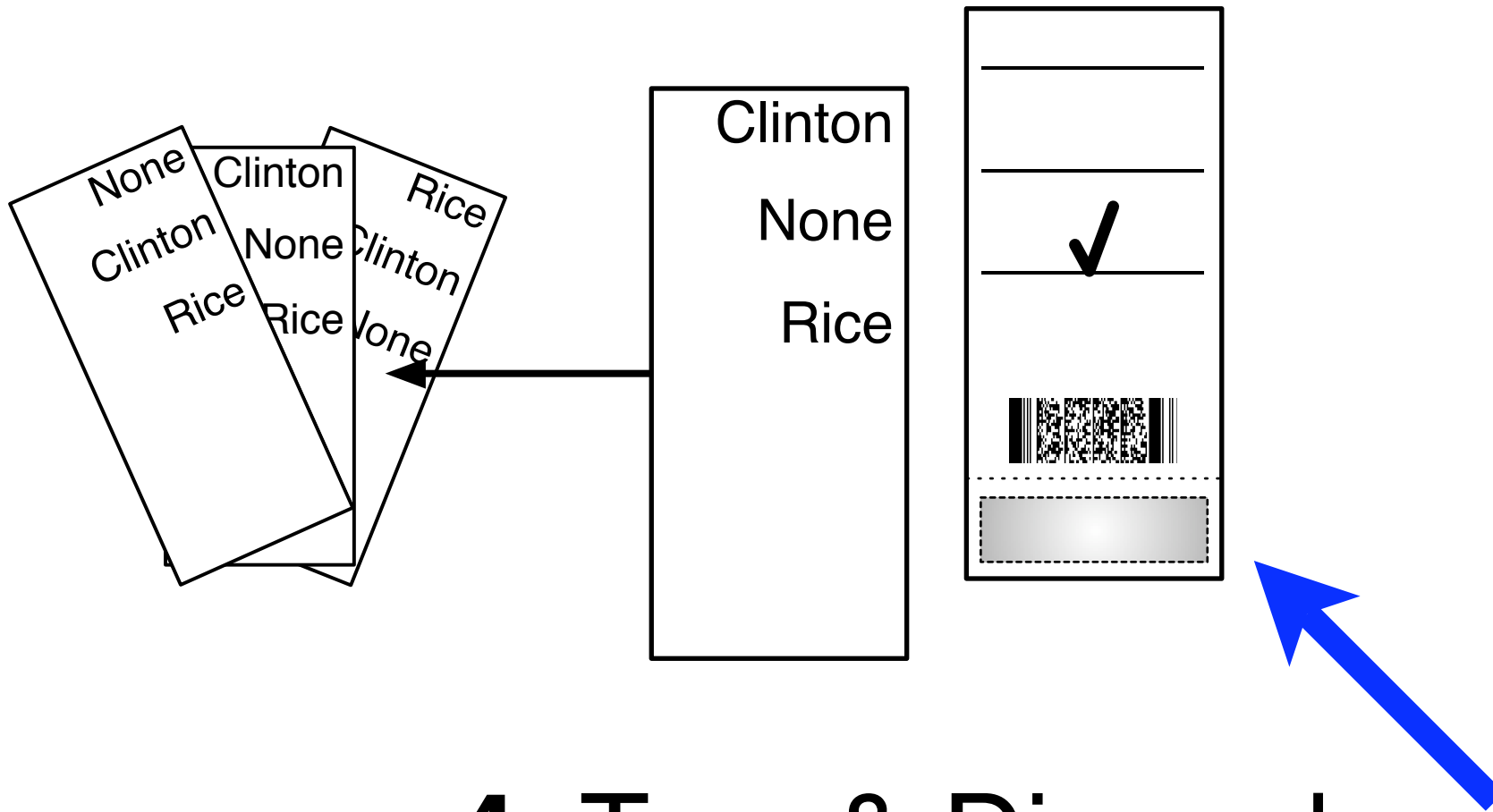
3. Vote.

In Private

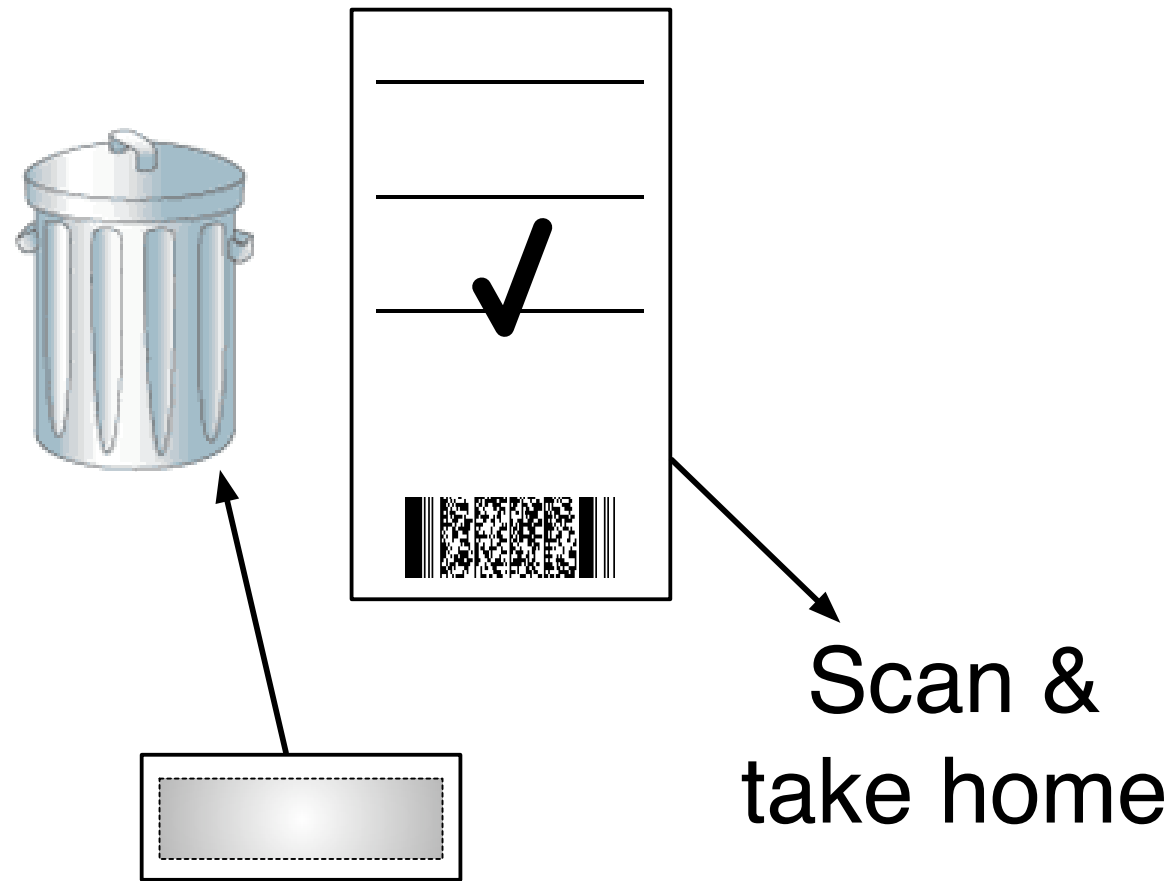


**4. Tear & Discard
left half of ballot.**

In Private




**4. Tear & Discard
left half of ballot.**



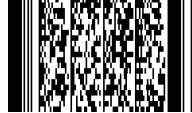
**5. Tear & Discard
scratch-off.**

Public Ballot Box


Alice

✓


Bridget

✓


Carol

✓


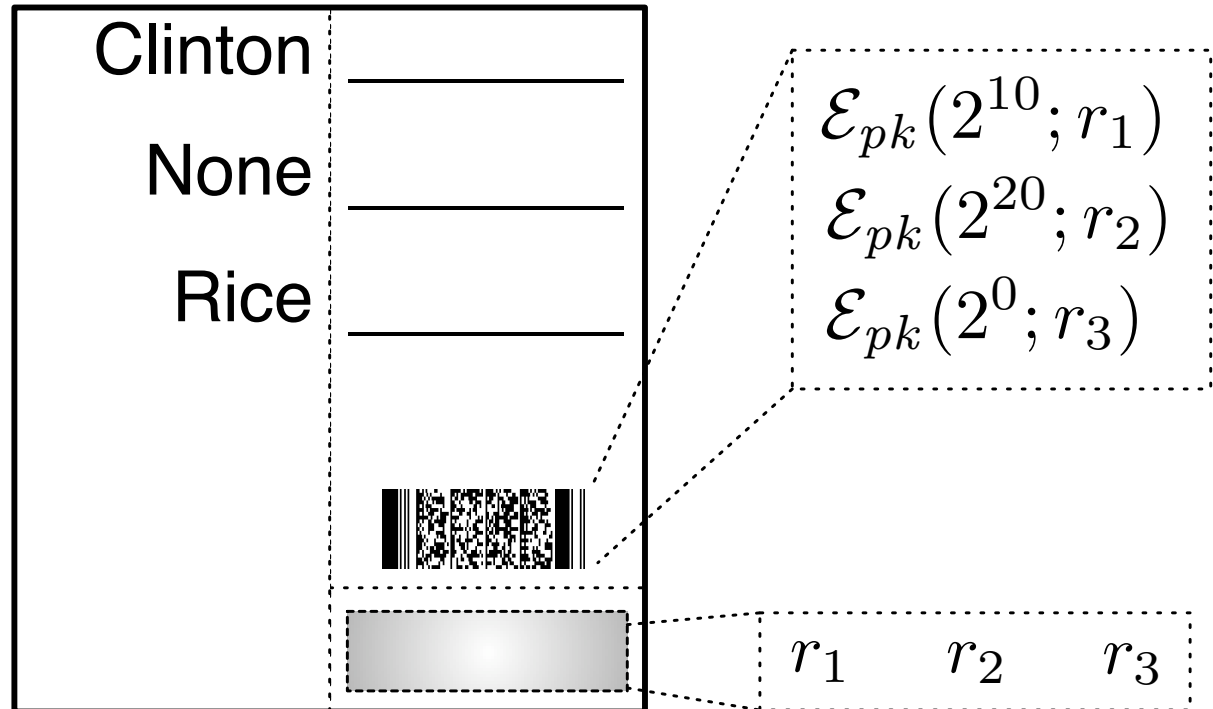
PARAMETERS

#1 - Rice

#2 - Clinton

#3 - None

M=10, Public Key = pk



Homomorphic Tallying

0001	0000	0000
------	------	------

Vote for Clinton

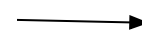
0000	0001	0000
------	------	------

Vote for Rice

0000	0000	0001
------	------	------

Vote for None

0004	0001	0008
------	------	------



Sample Tally

[B+2001, P1999]

Scratch & Vote is **one** system.
There are many others.

In Summary

In Summary

- End-to-End verification

In Summary

- End-to-End verification
- Secrecy and Verifiability **are** reconcilable

In Summary

- End-to-End verification
- Secrecy and Verifiability **are** reconcilable
- Simplicity & Practicality are well on their way...

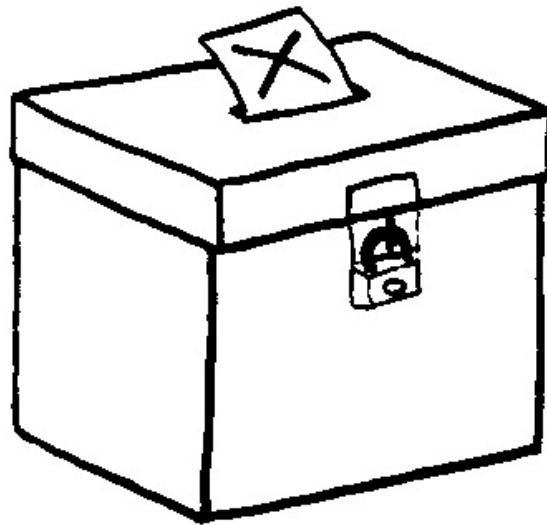
In Summary

- End-to-End verification
- Secrecy and Verifiability **are** reconcilable
- Simplicity & Practicality are well on their way...
- The Paper Trail is not enough.
Hand-Counted Ballots are not enough.

In Summary

- End-to-End verification
- Secrecy and Verifiability **are** reconcilable
- Simplicity & Practicality are well on their way...
- The Paper Trail is not enough.
Hand-Counted Ballots are not enough.
- **Open-Audit Voting**: let anyone verify.

Questions?



Practical Considerations

5 questions, 5 options per question.

- *Ballot Verification*: less than a second.
- *Barcode Encoding*: PDF417 open standard.
- *Barcode Size*: 10 square inches of barcode for a full sheet visual ballot.
- *ProofTime*: ~3 seconds per ballot.