WPES

Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting

Ben Adida

Harvard Engineering and Applied Sciences

Ronald L. Rivest

MIT

30 October 2006

the ONION
America's Finest News Source

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.

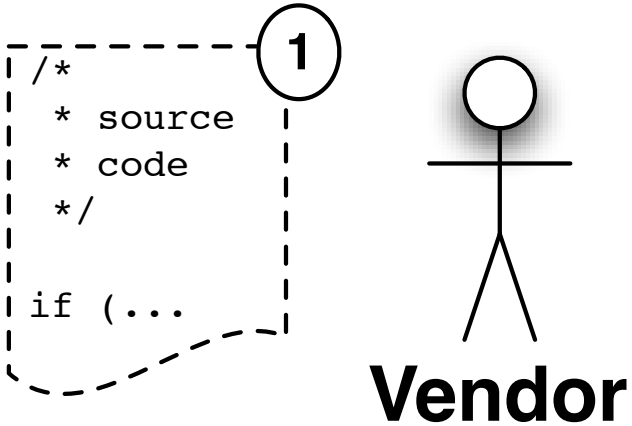
The Next Harvard Pres!

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

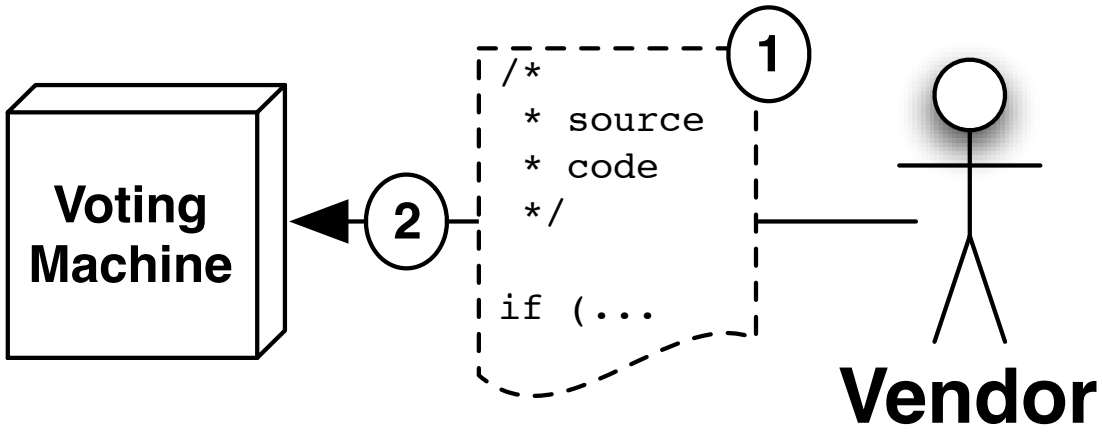
US News & World Report/Washington Whispers | Paul Bedard | Posted September 10, 2006 02:43 PM

Chain of Custody

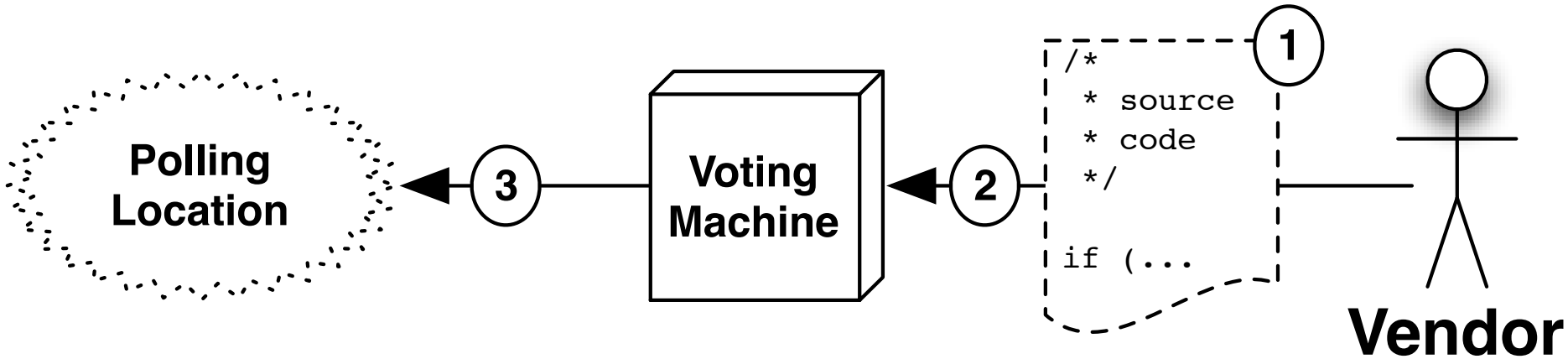
Chain of Custody



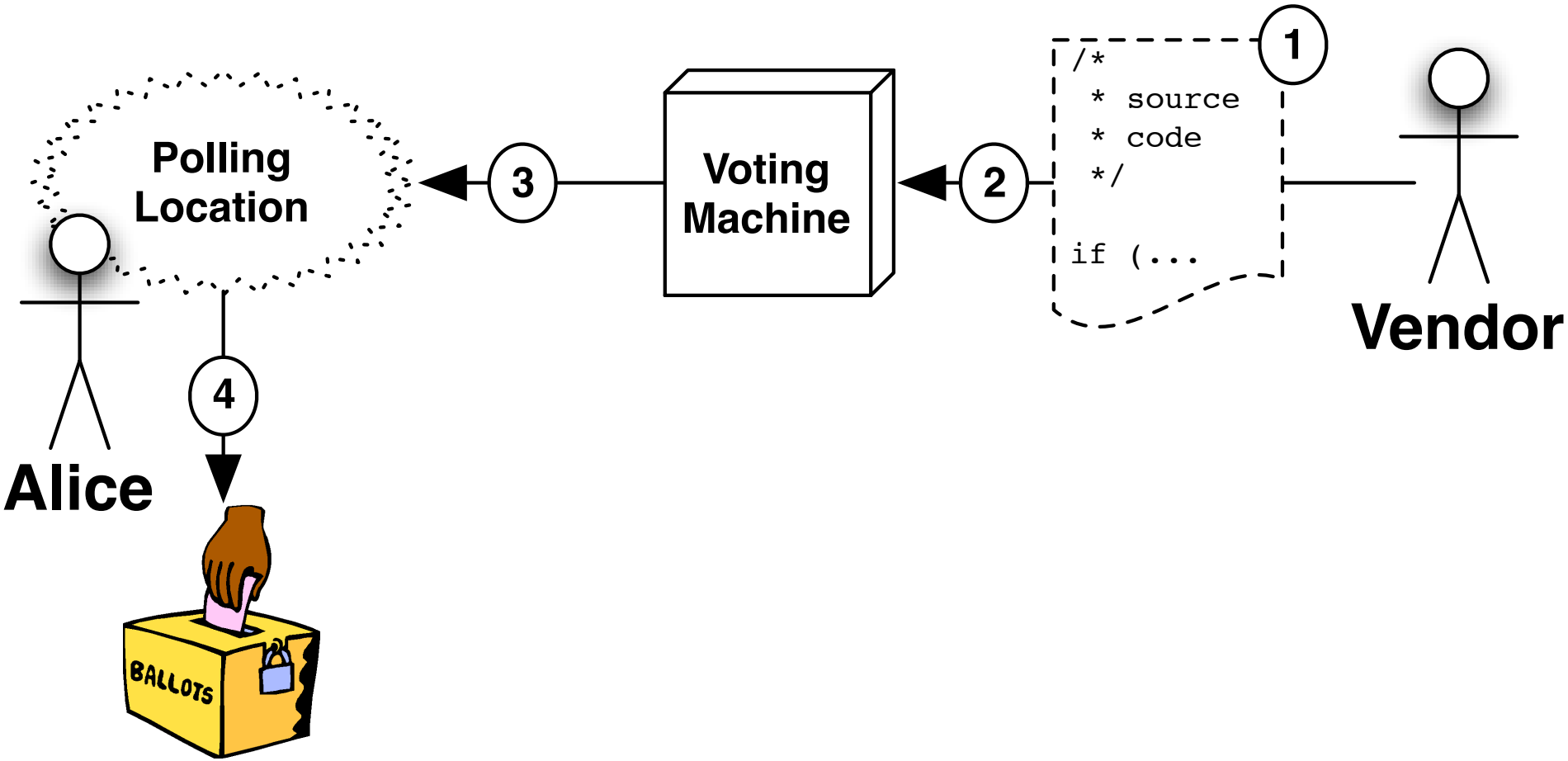
Chain of Custody



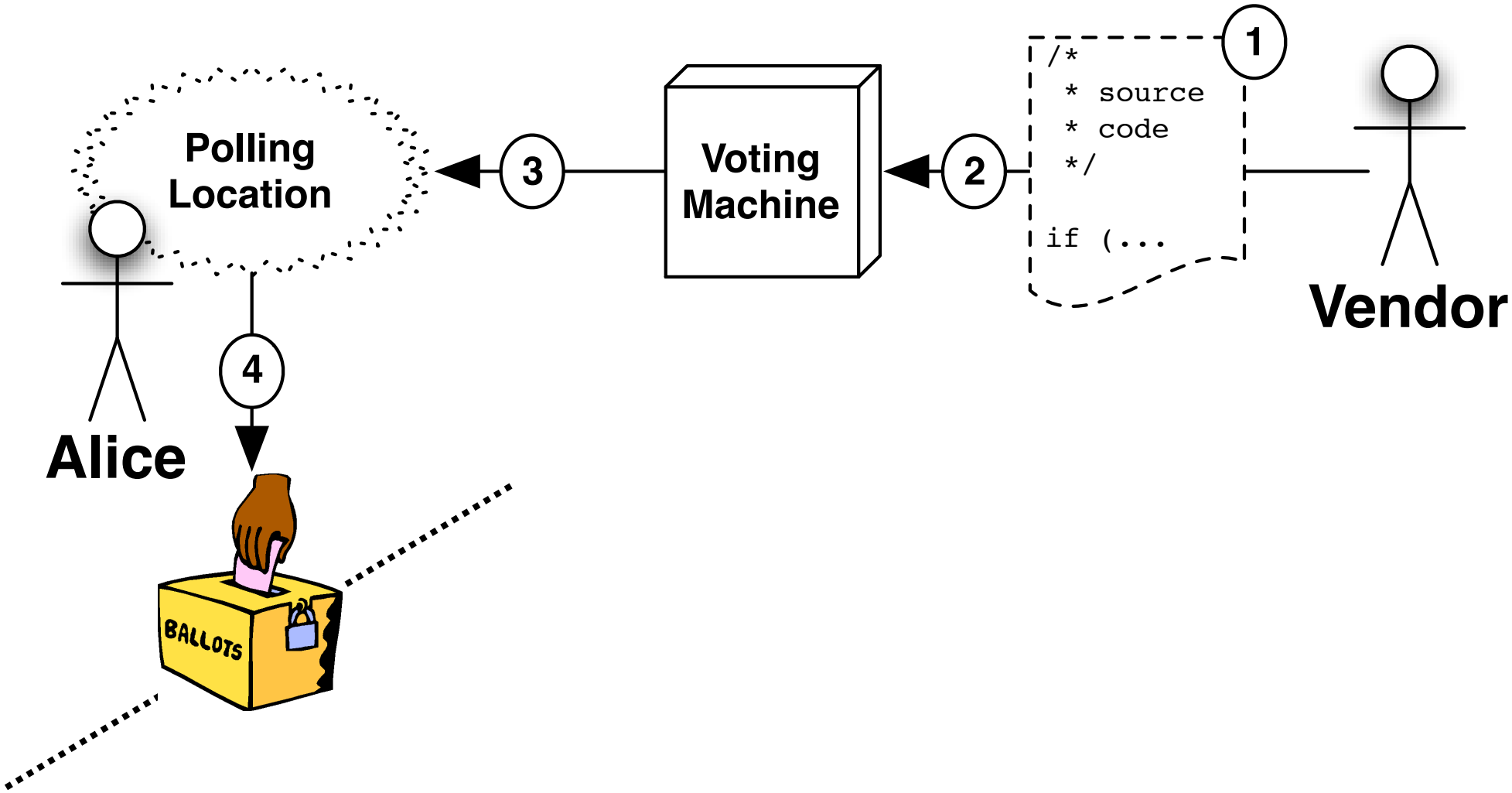
Chain of Custody



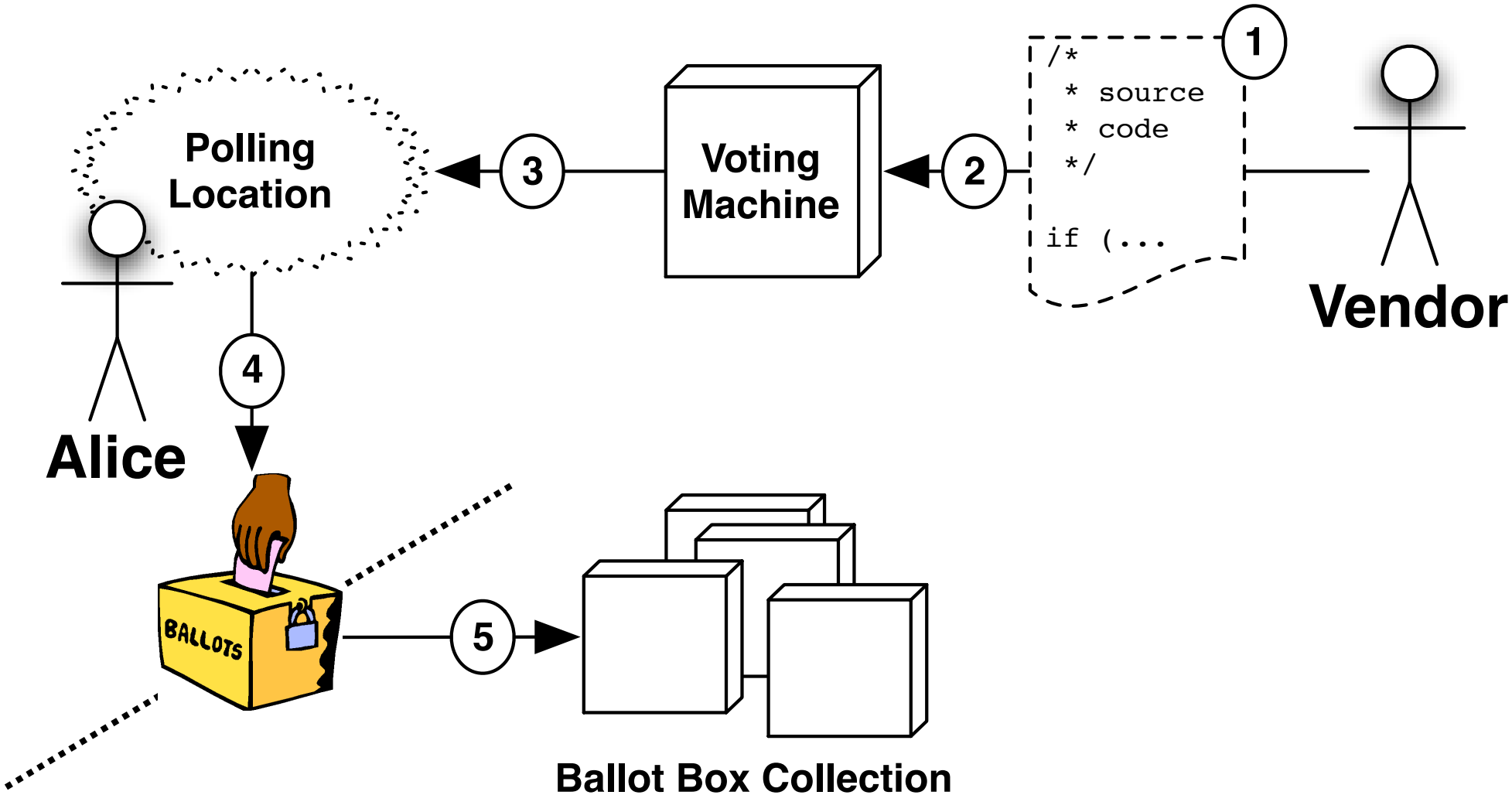
Chain of Custody



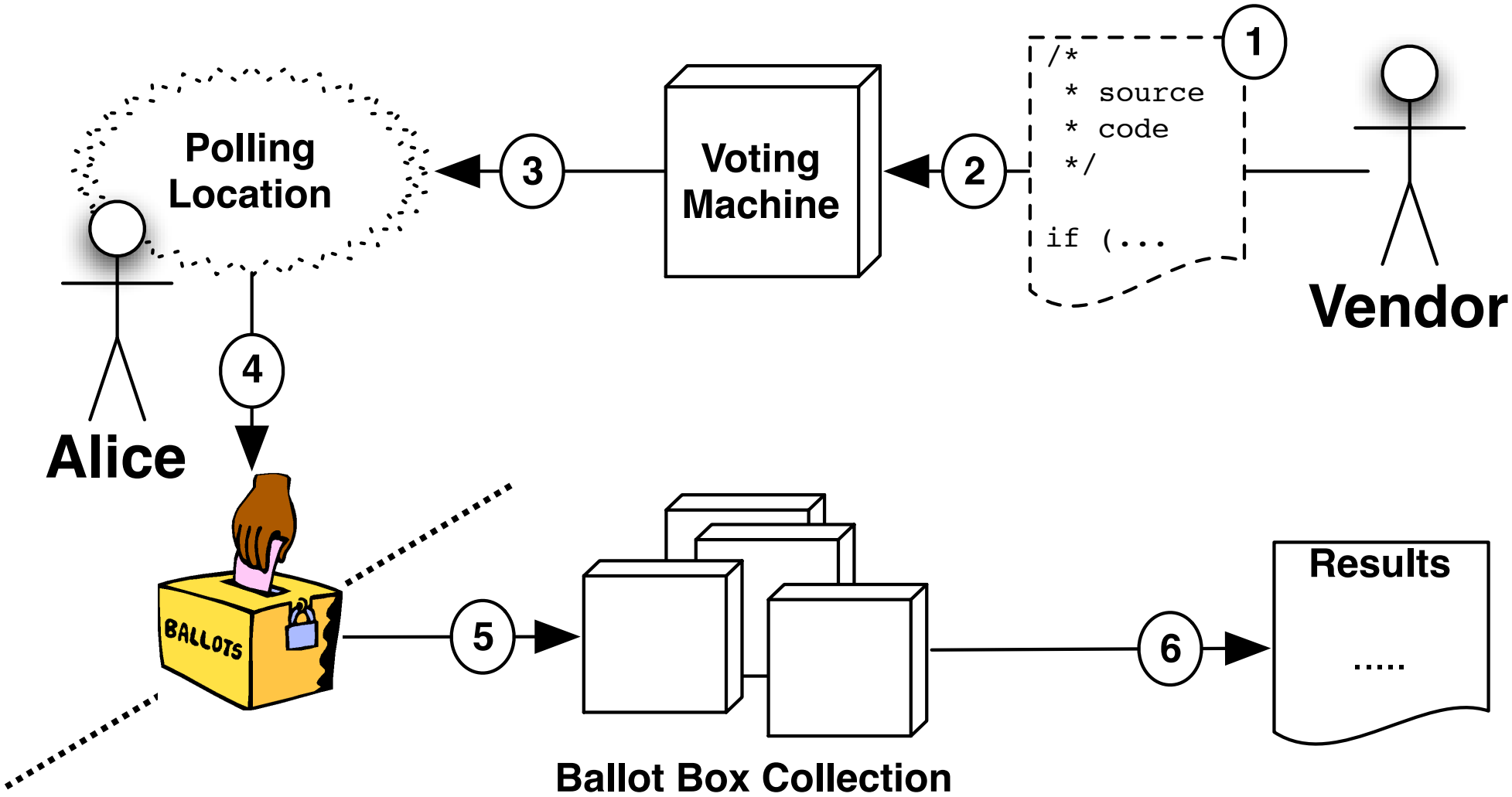
Chain of Custody



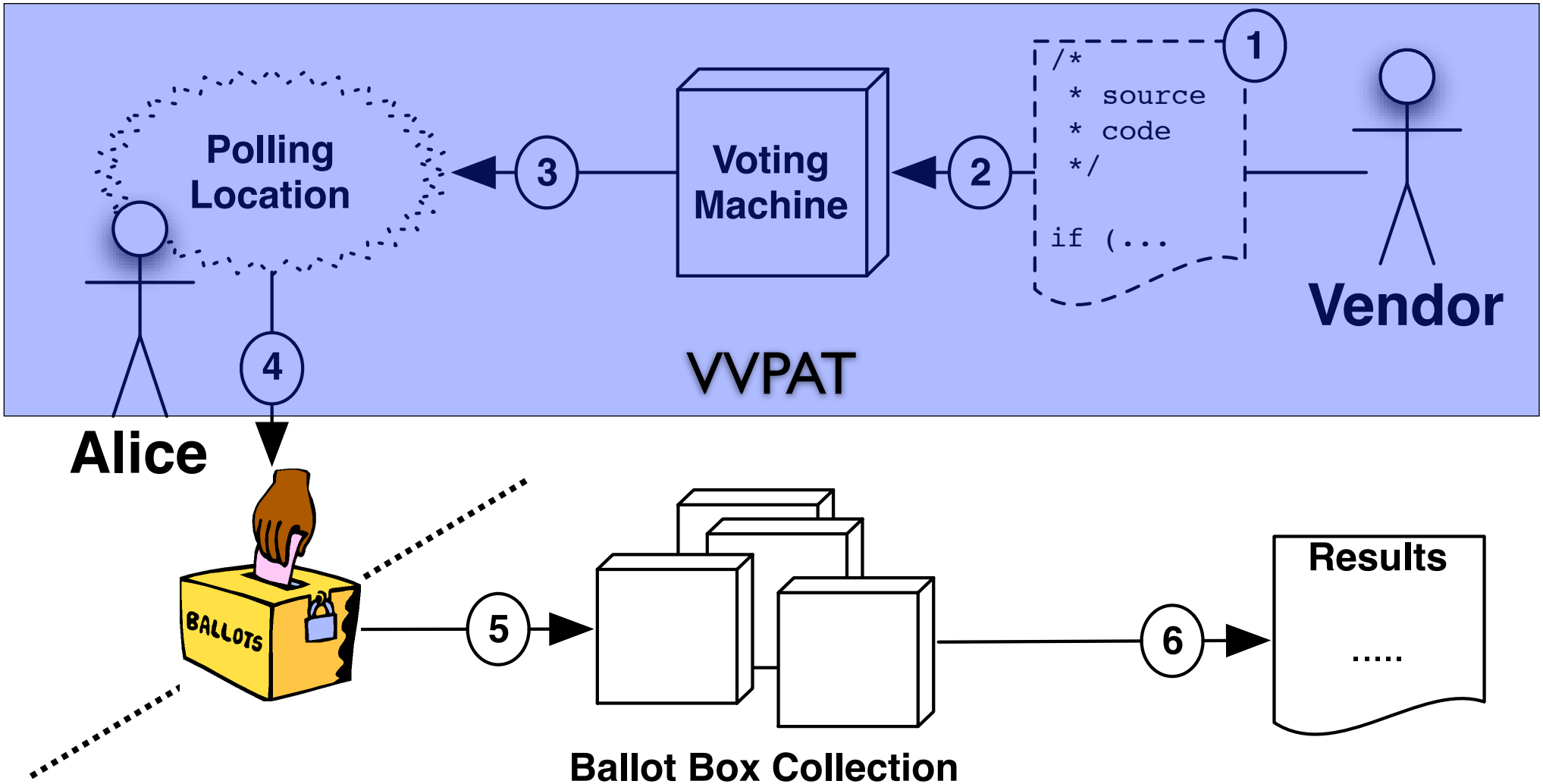
Chain of Custody



Chain of Custody

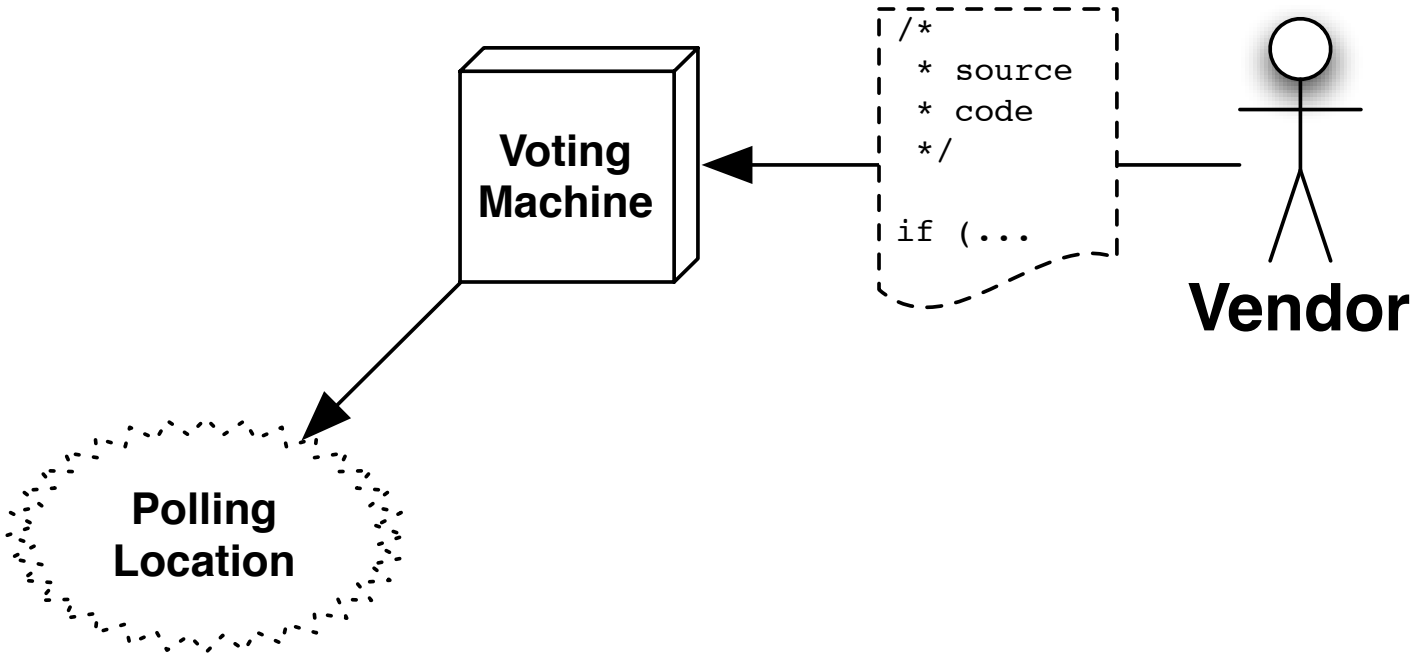


Chain of Custody

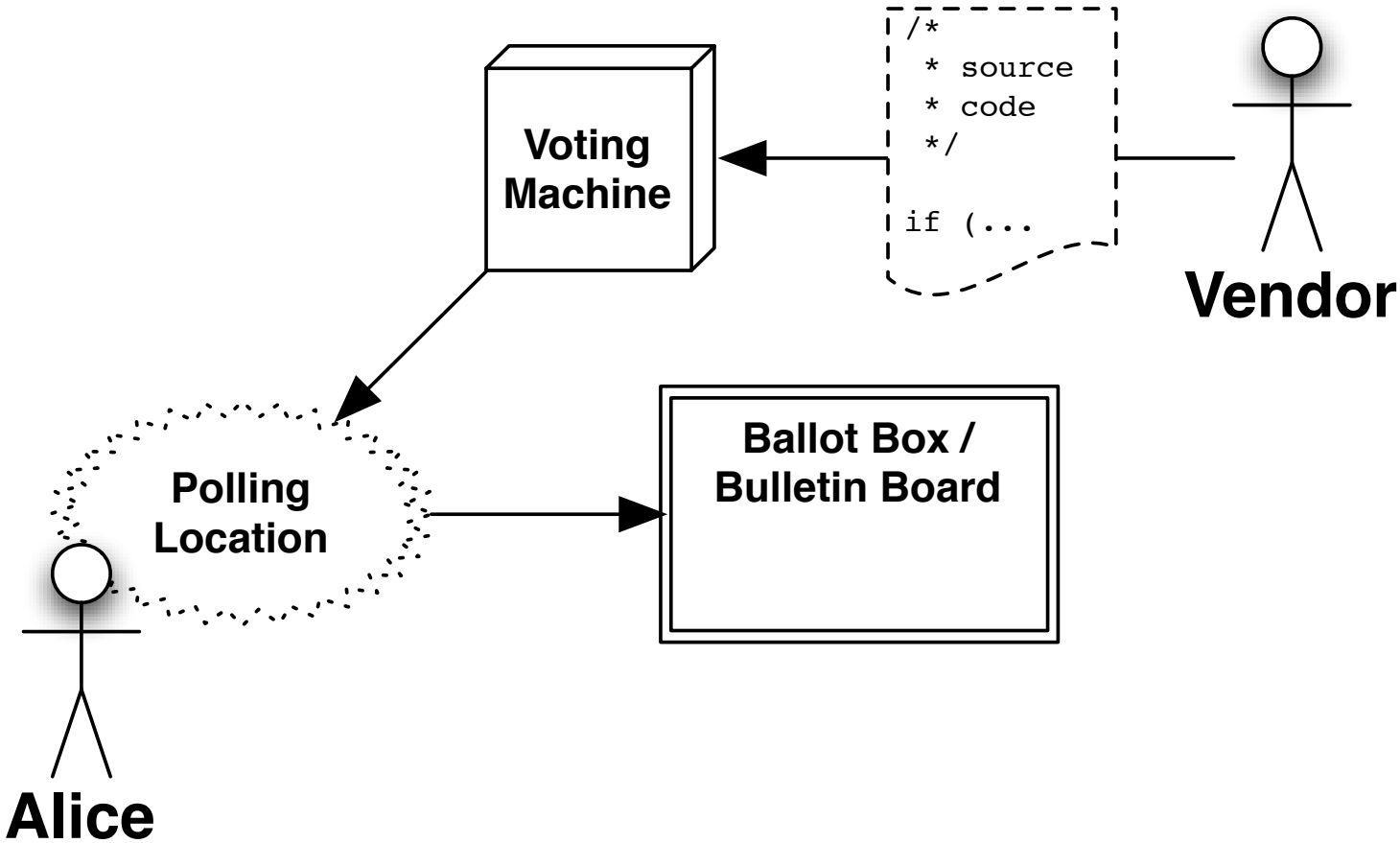


End-to-End

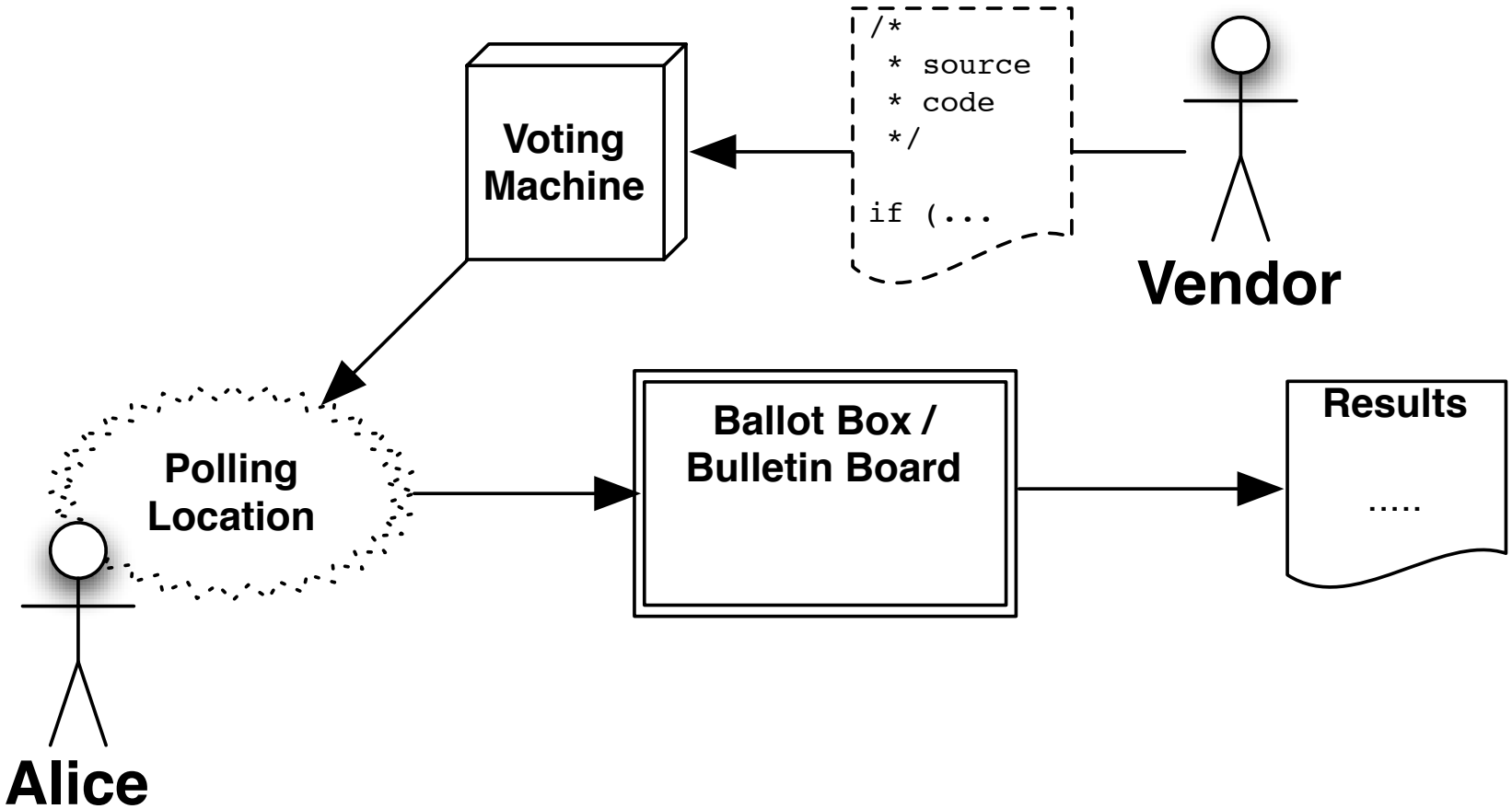
End-to-End



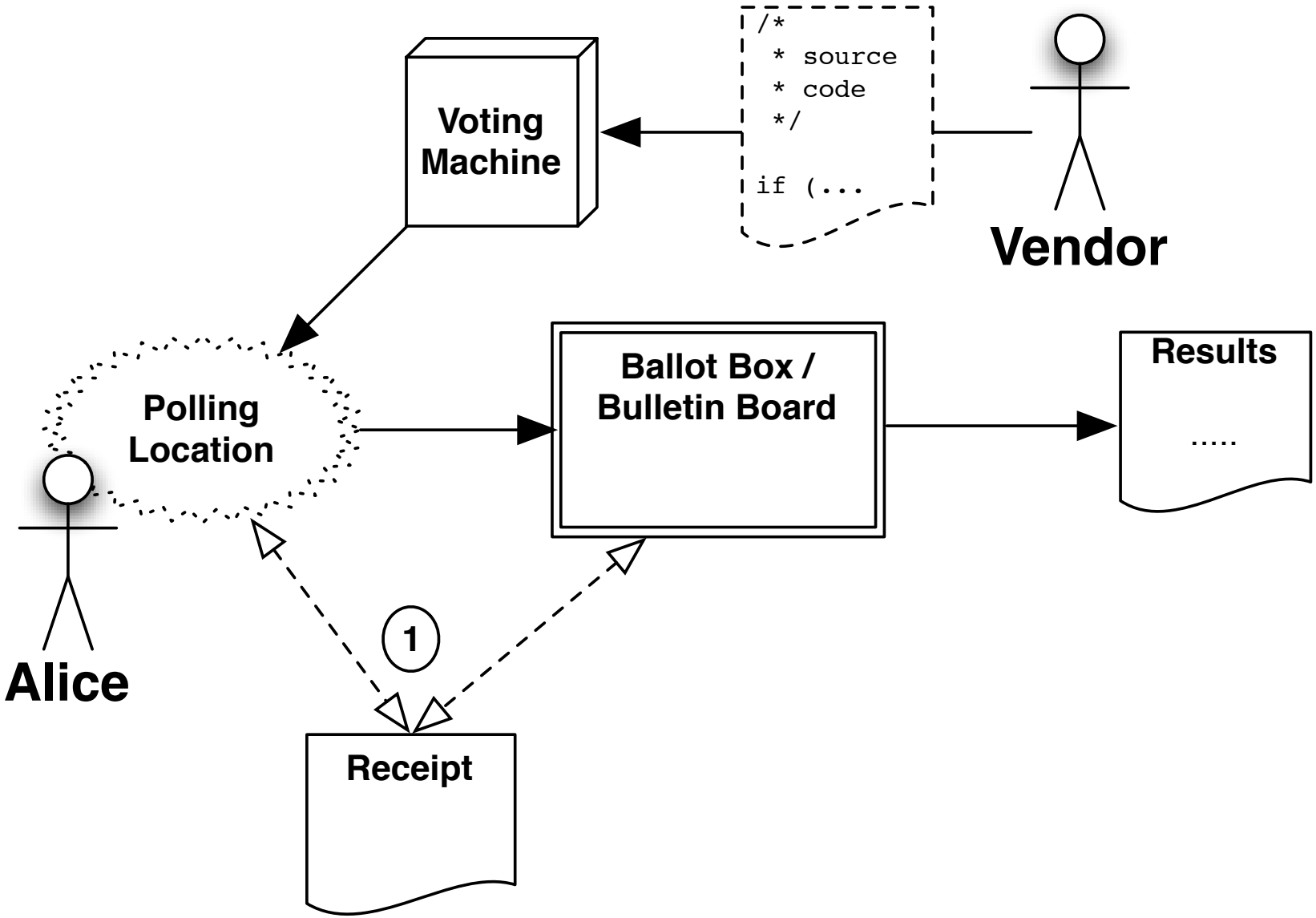
End-to-End


/*
* source
* code
*/
if (...
Voting Machine
Vendor
Polling Location
Ballot Box / Bulletin Board
Alice

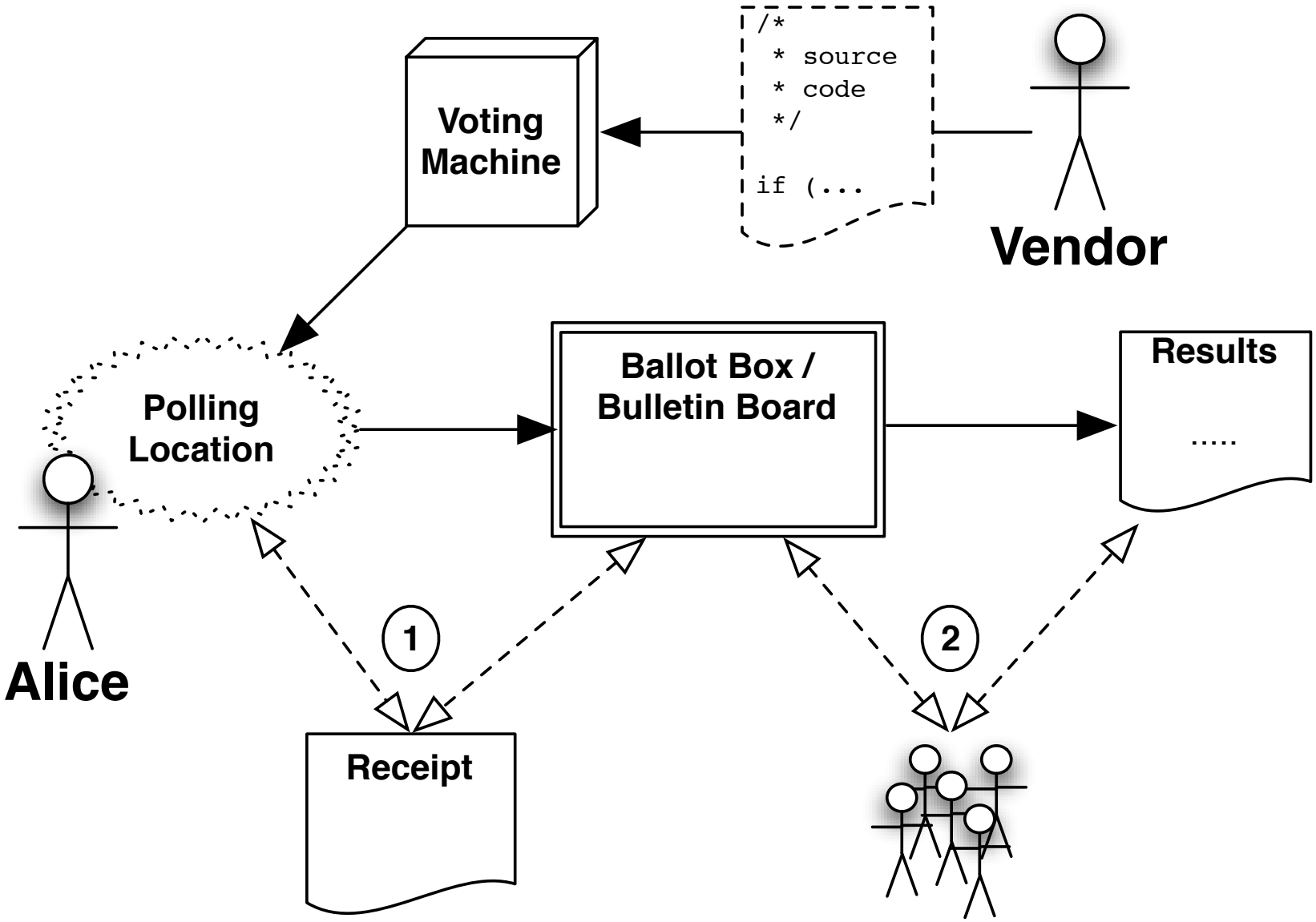
End-to-End


/*
* source
* code
*/
if (...
Voting Machine
Vendor
Polling Location
Ballot Box / Bulletin Board
Results
.....
Alice

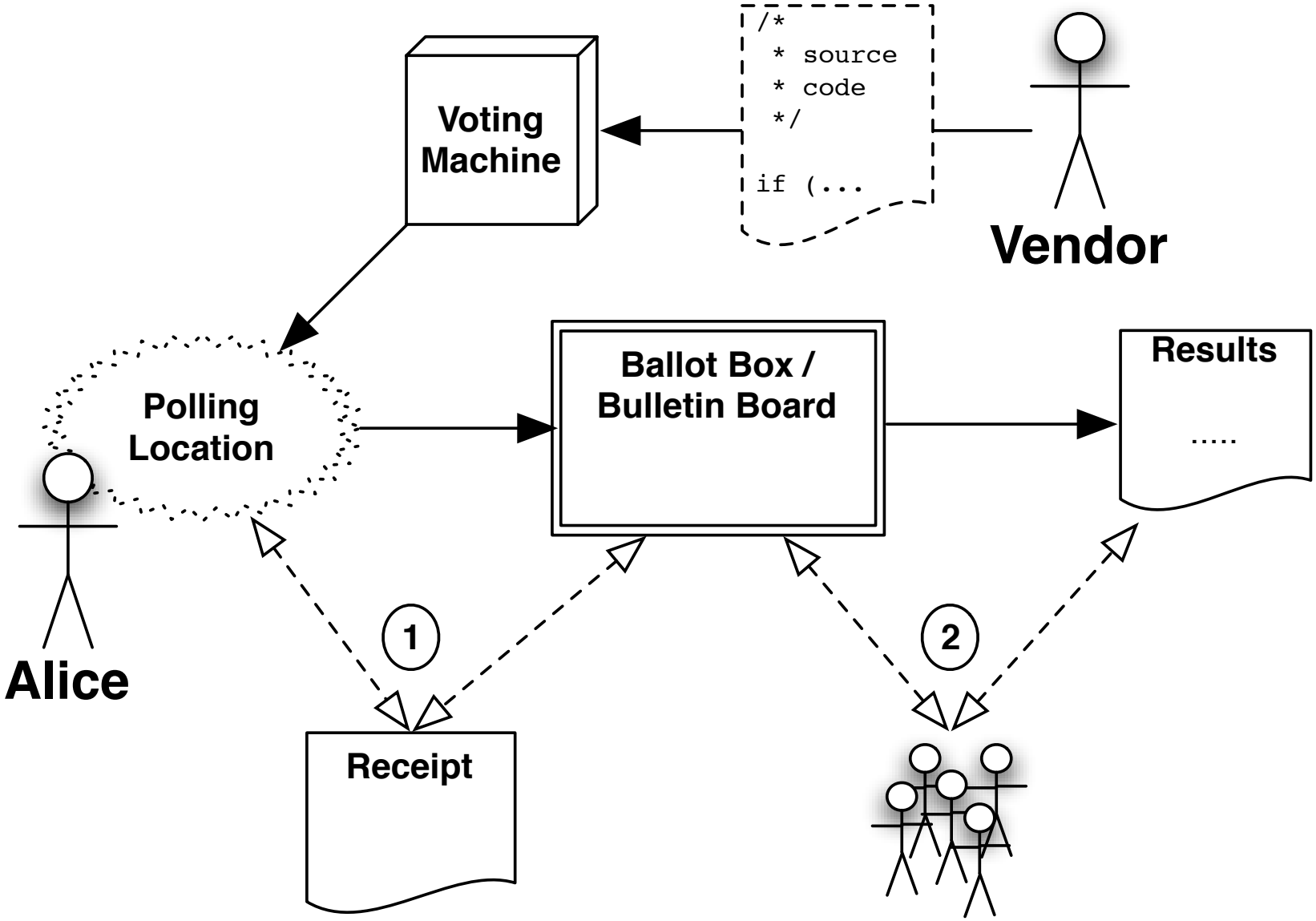
End-to-End


/*
* source
* code
*/
if (...
Voting Machine
Vendor
Polling Location
Ballot Box / Bulletin Board
Results
.....
Alice
1
Receipt

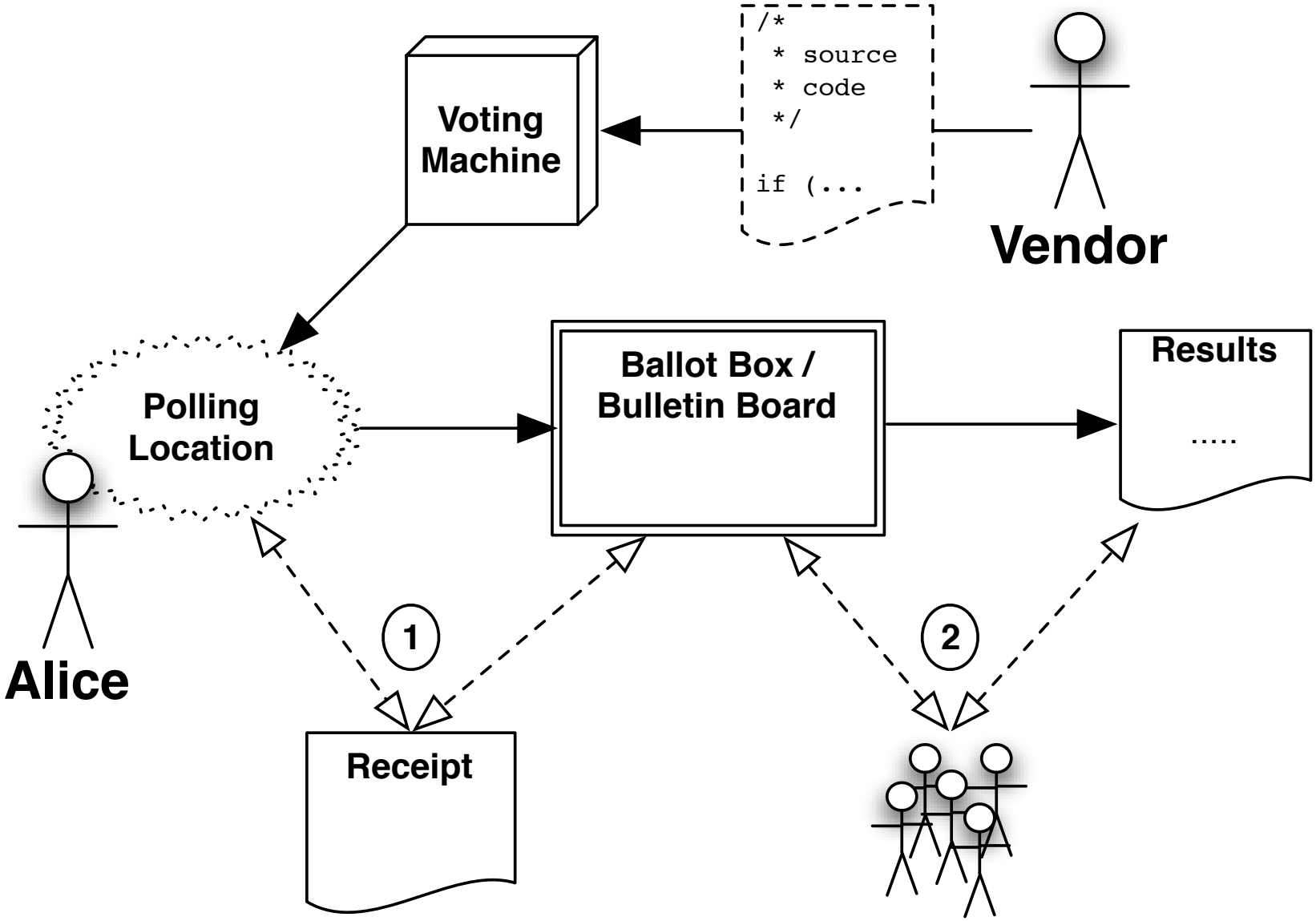
End-to-End


/*
* source
* code
*/
if (...
Voting Machine
Vendor
Polling Location
Ballot Box / Bulletin Board
Results
.....
Alice
1
2
Receipt

Cryptographic Voting



Open-Audit Voting



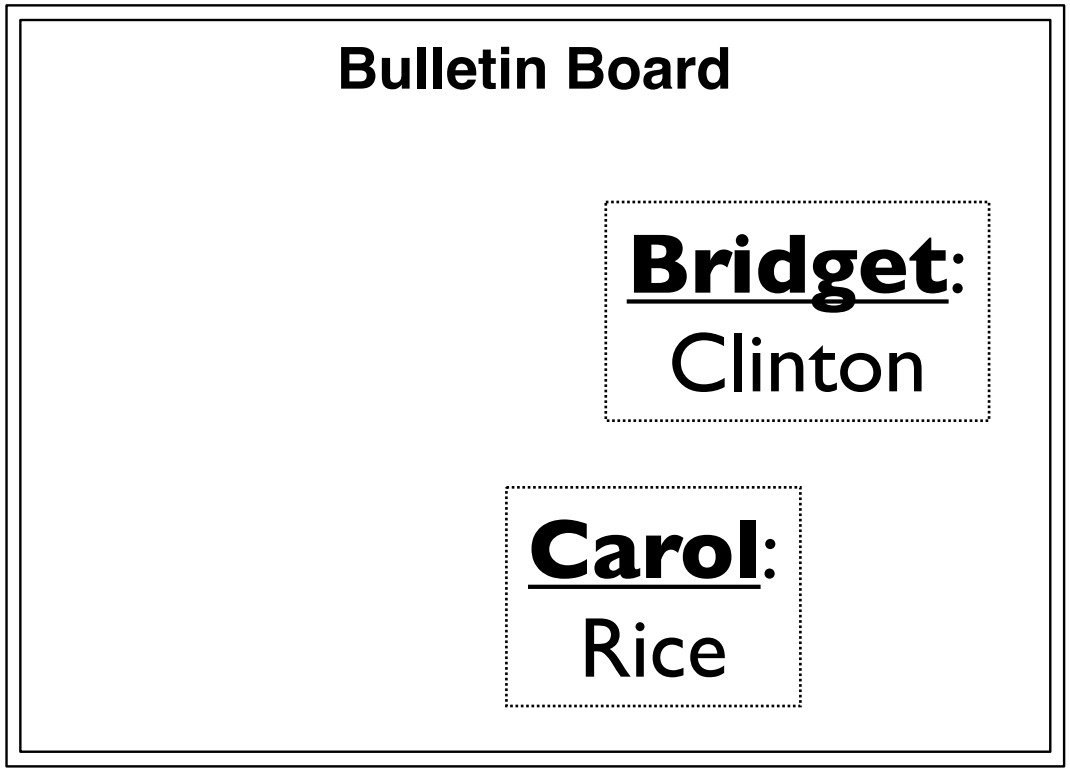
Properties of OAV

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

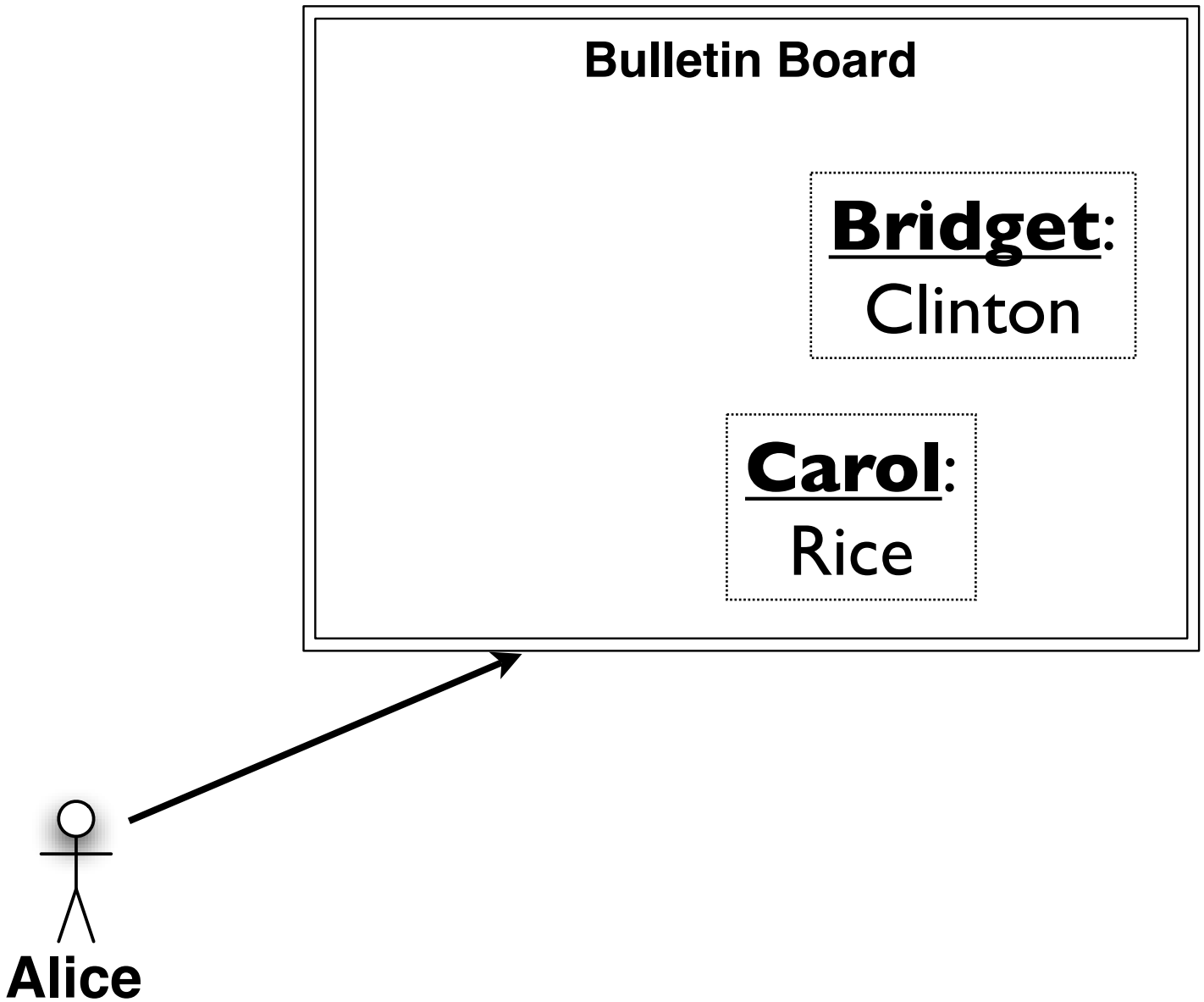
(2) **Everyone** verifies **tallying**.

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

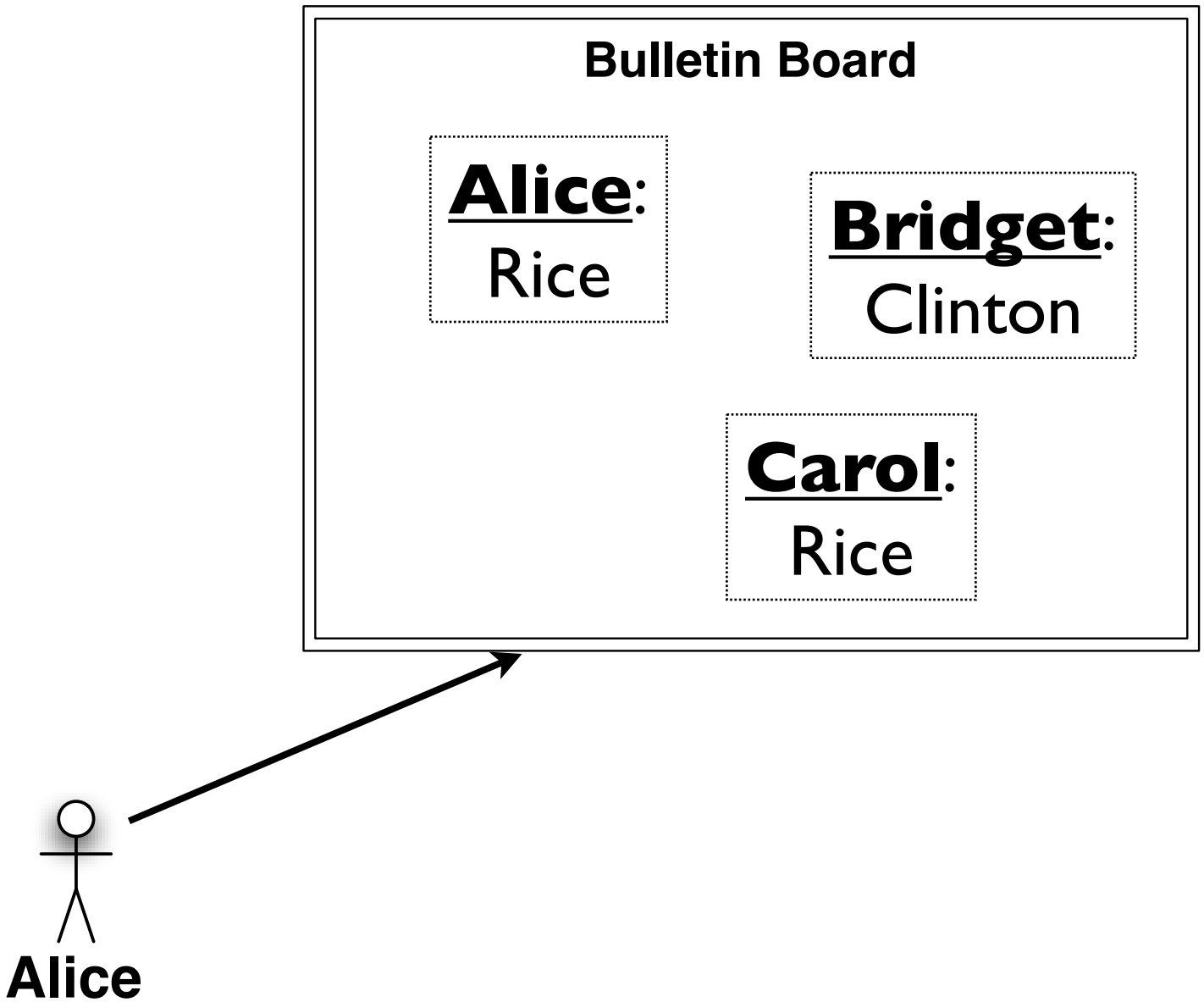
A Bulletin Board



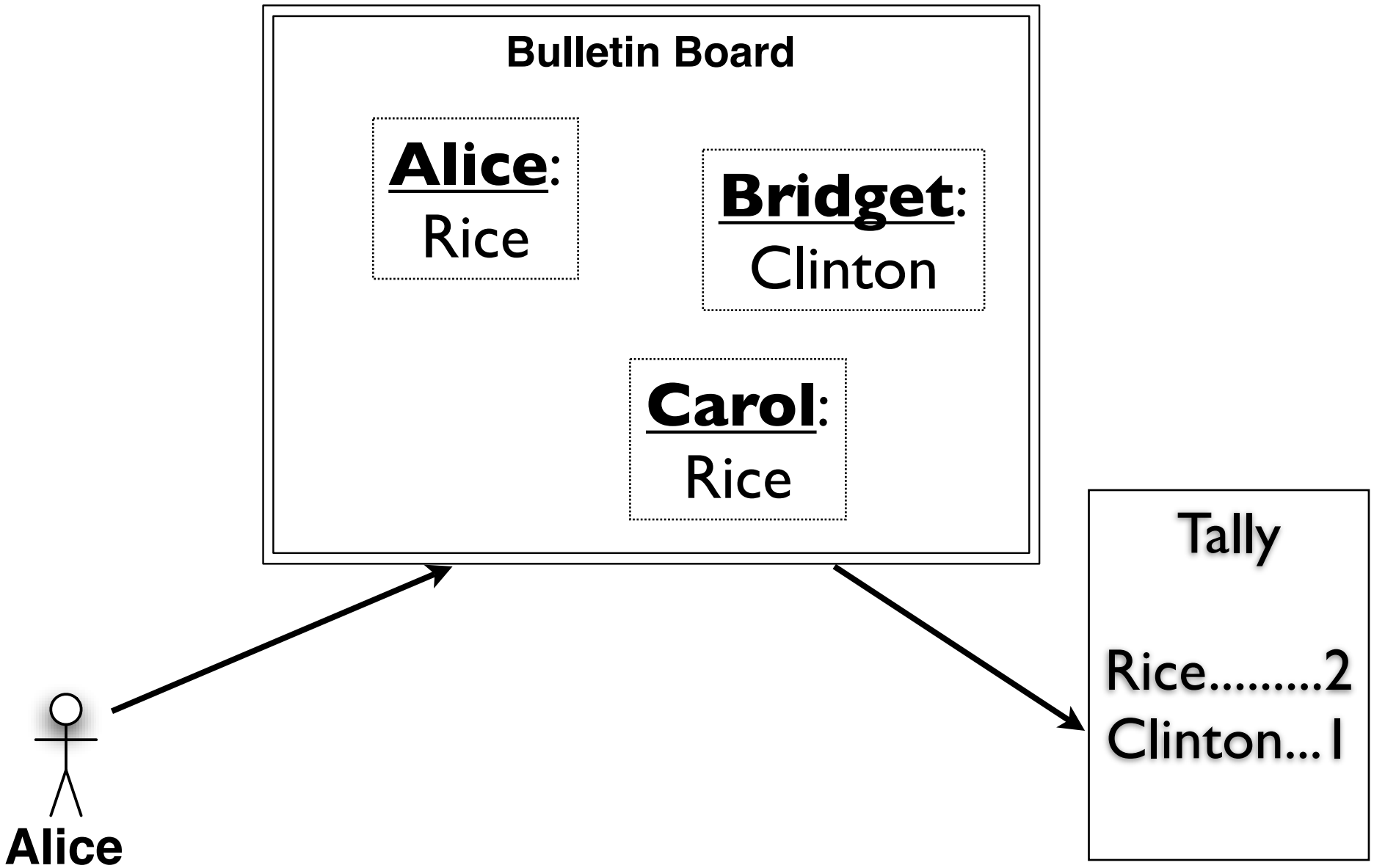
A Bulletin Board



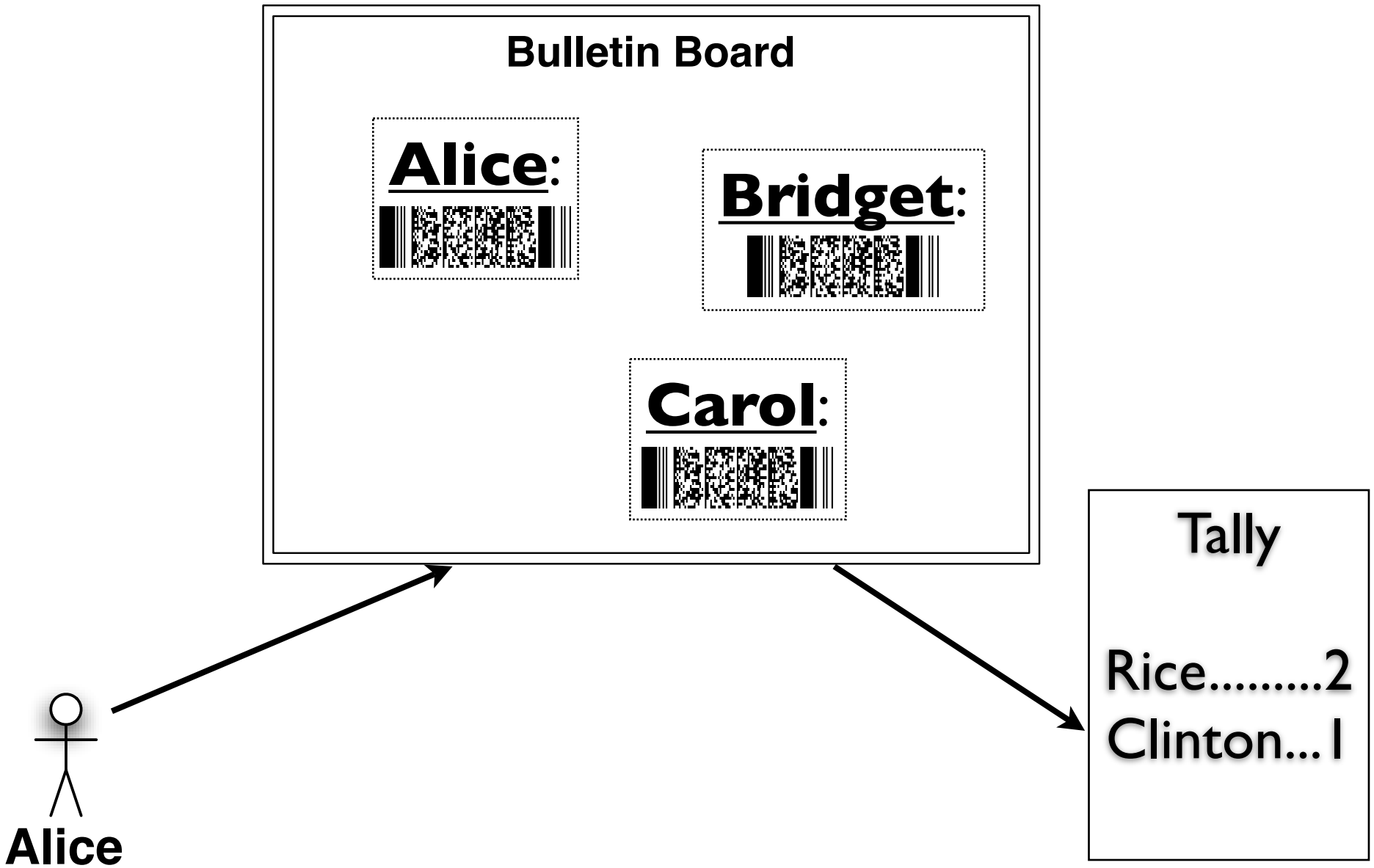
A Bulletin Board

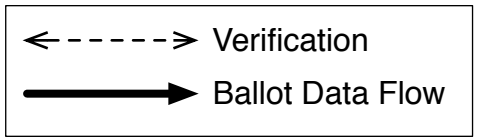


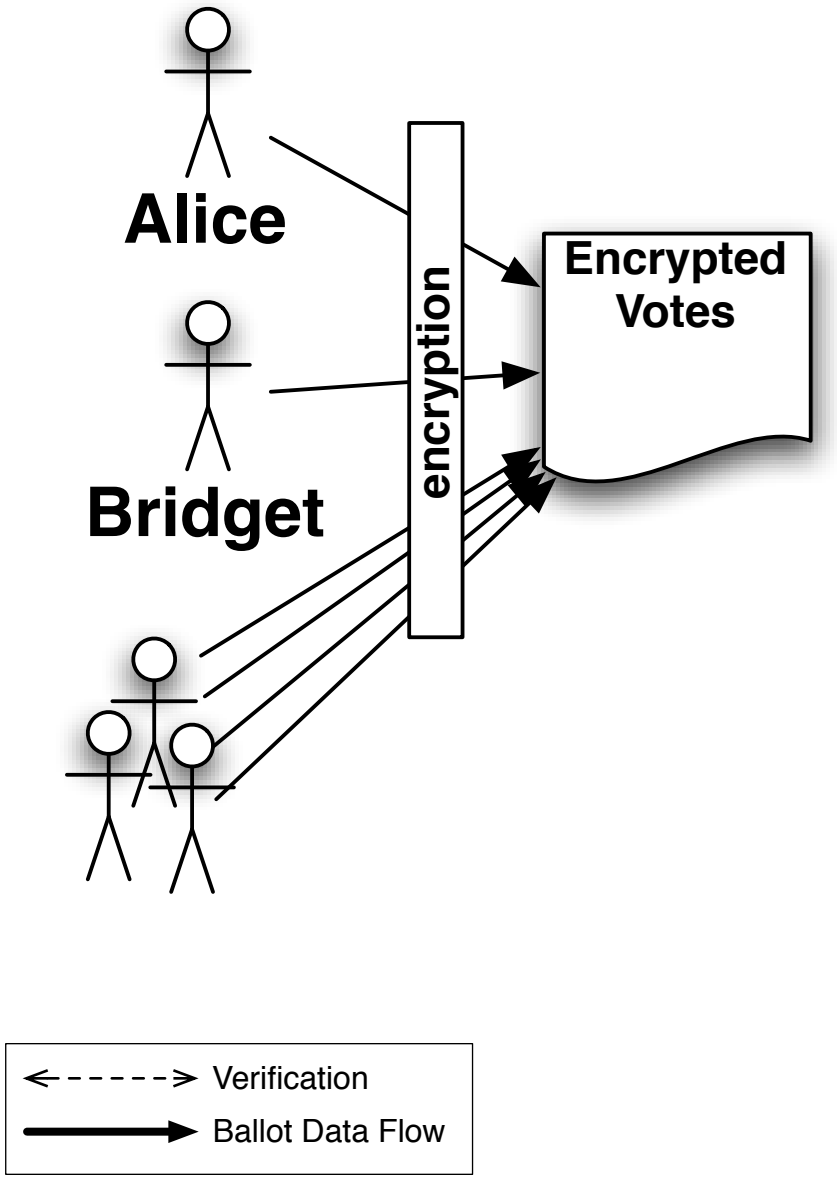
A Bulletin Board

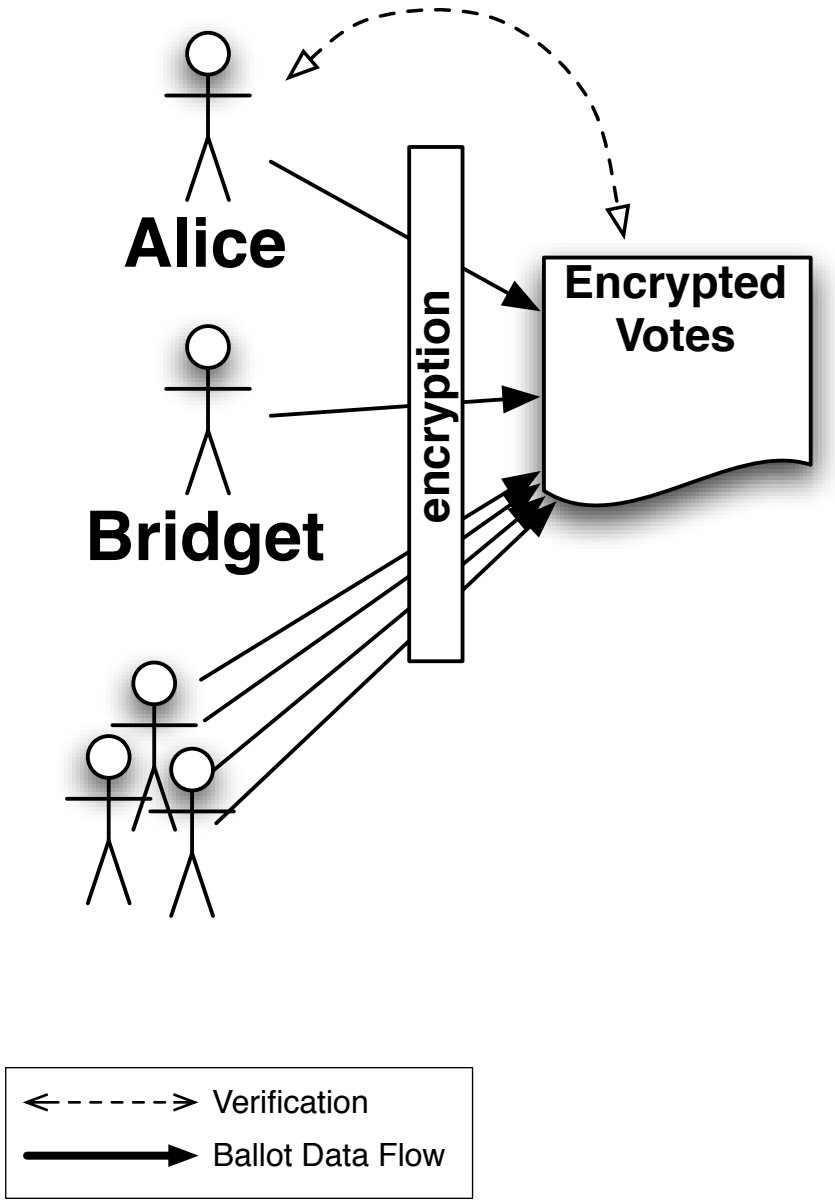


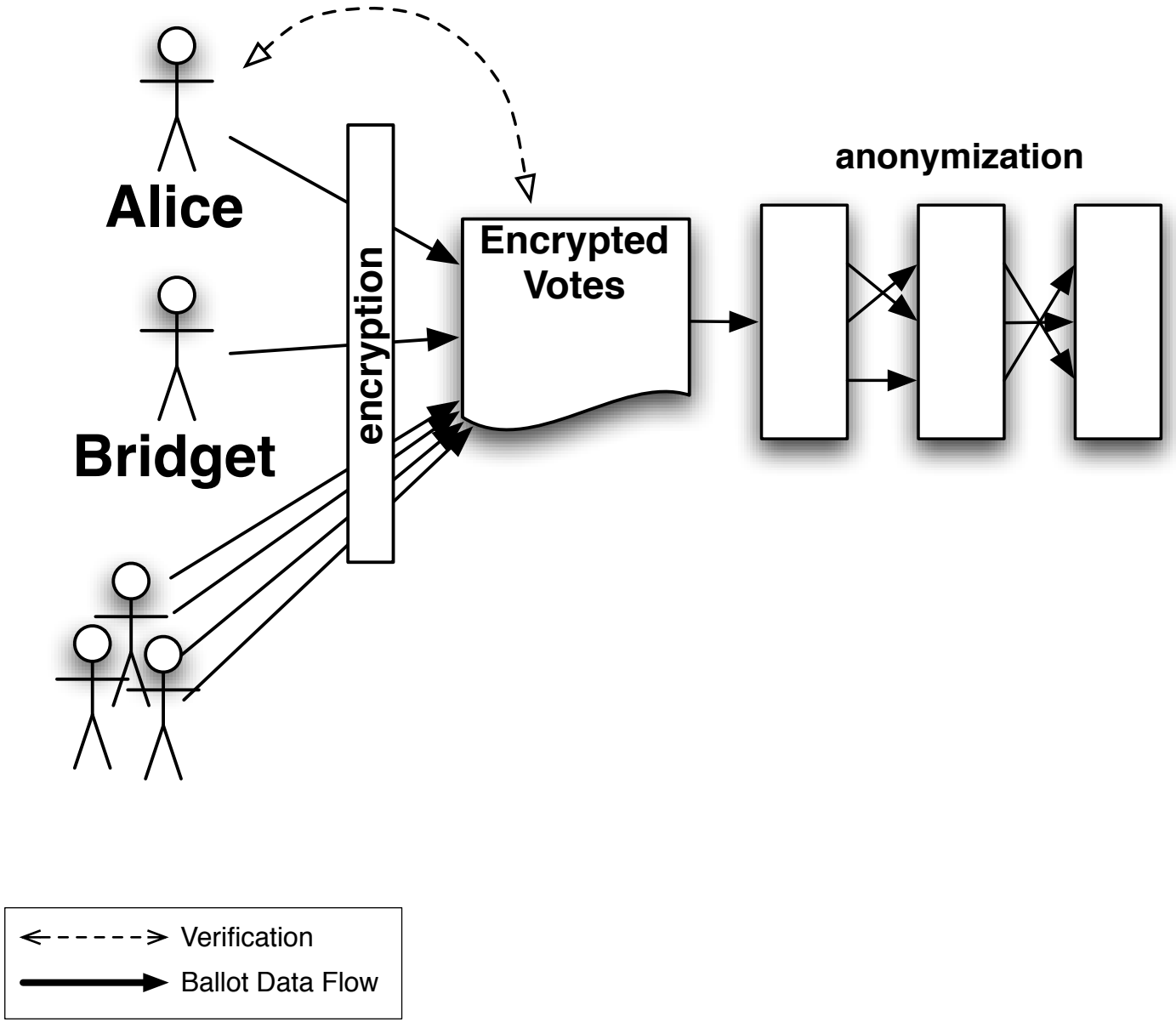
An *Encrypted* Bulletin Board

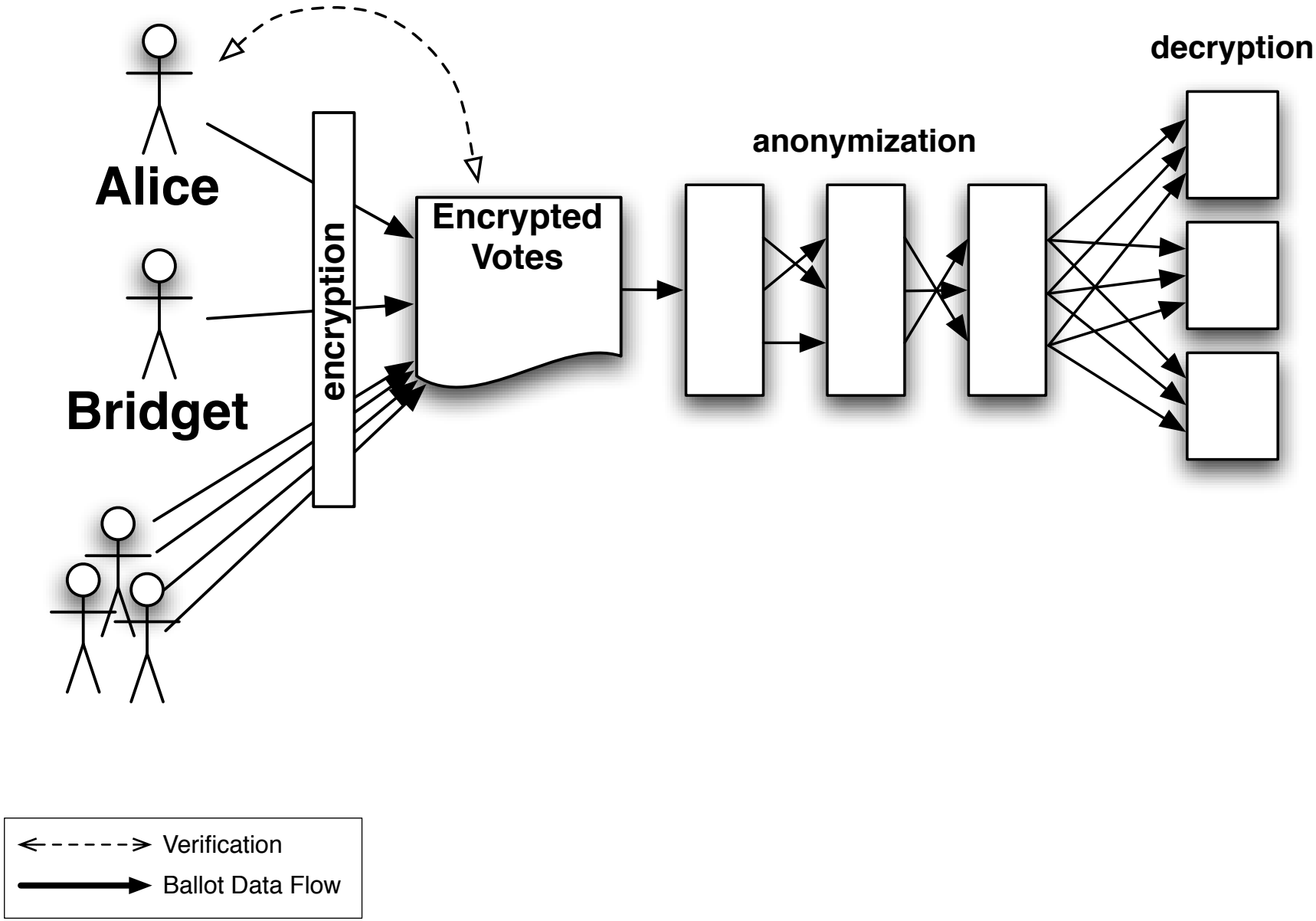


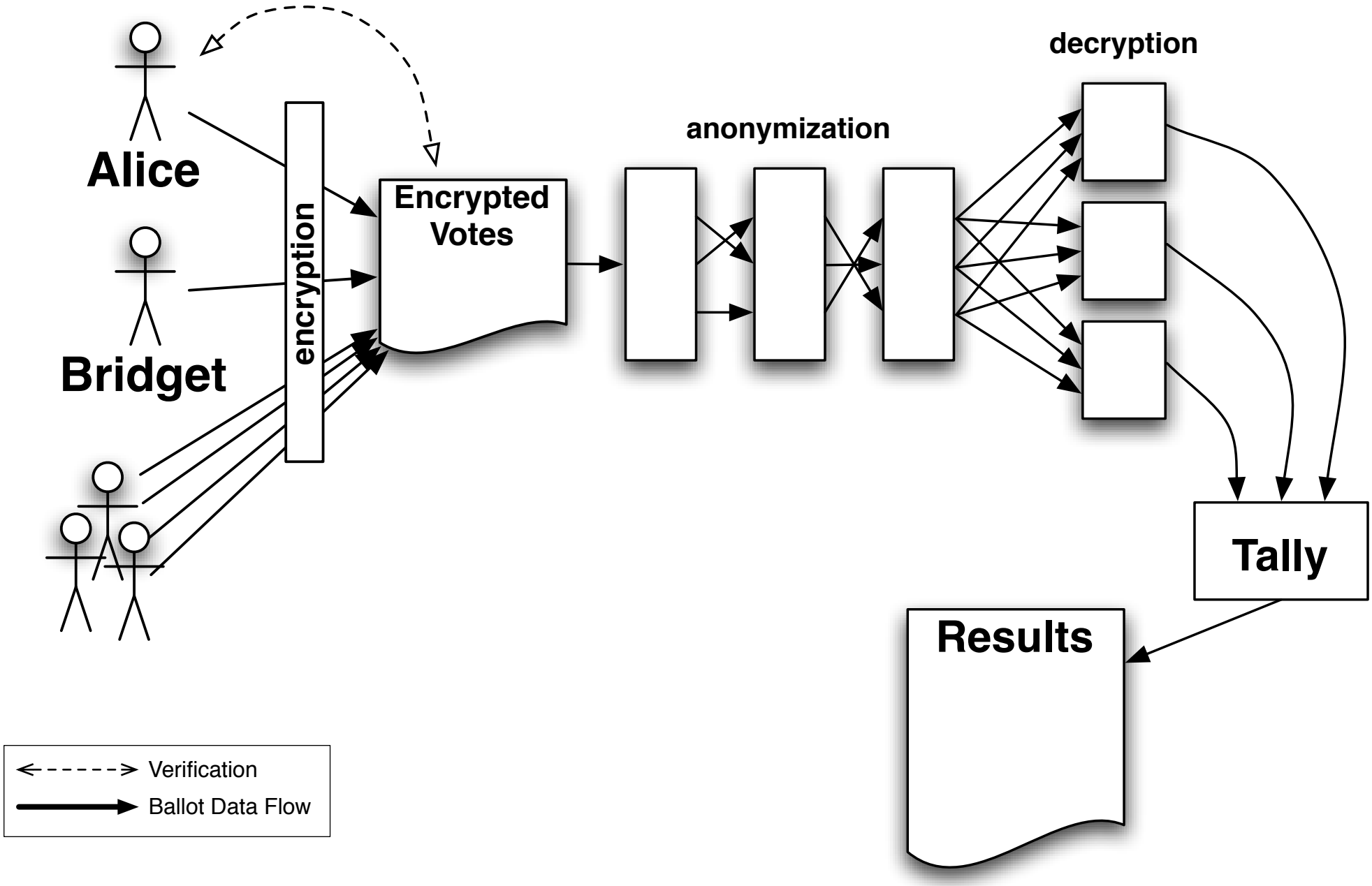

Verification
Ballot Data Flow

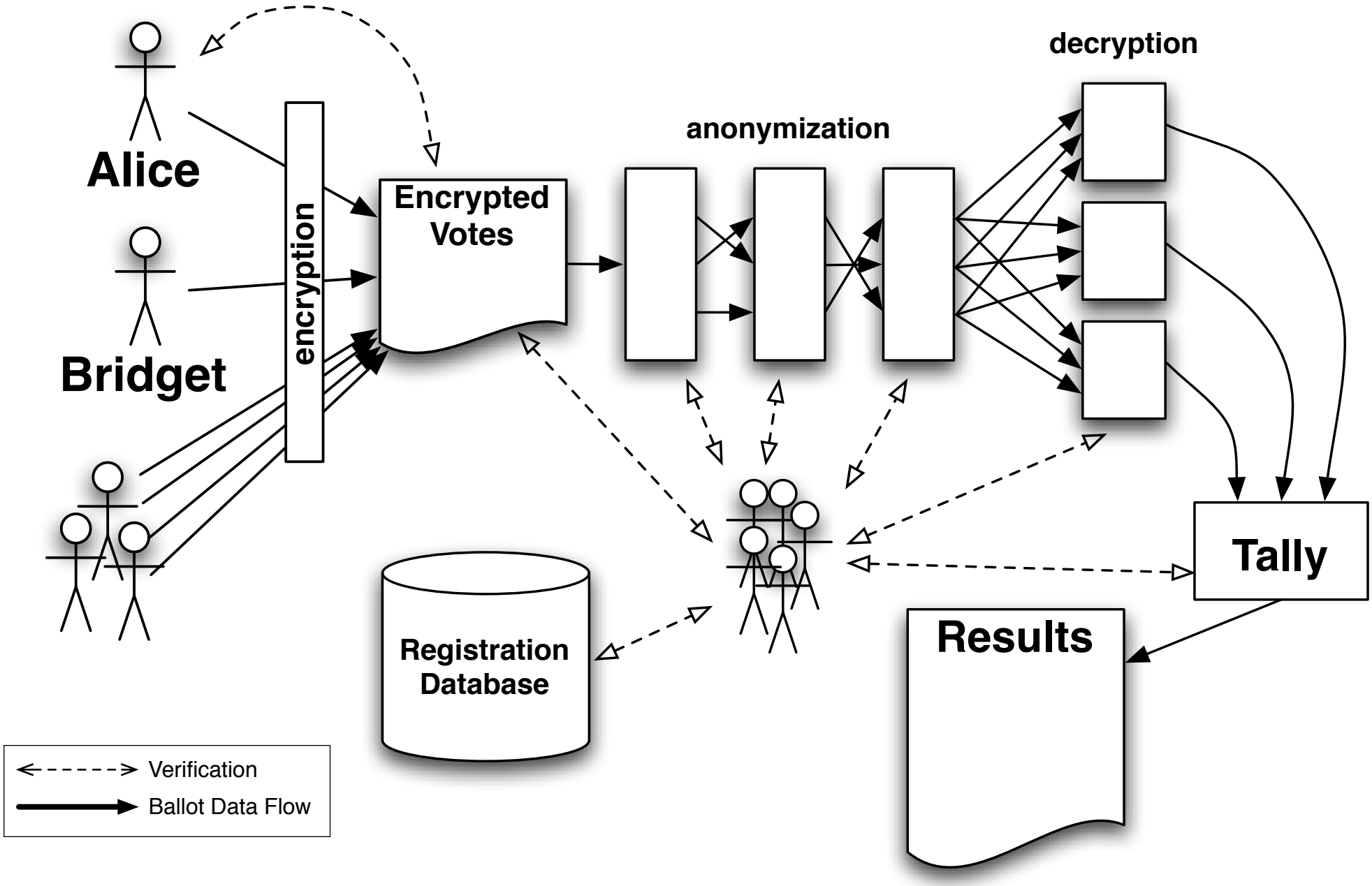

Alice
Bridget
encryption
Encrypted Votes
Verification
Ballot Data Flow


Alice
Bridget
encryption
Encrypted Votes
Verification
Ballot Data Flow


Alice
Bridget
encryption
Encrypted Votes
anonymization
Verification
Ballot Data Flow


Alice
Bridget
encryption
Encrypted Votes
anonymization
decryption
Verification
Ballot Data Flow


Alice
Bridget
encryption
Encrypted Votes
anonymization
decryption
Tally
Results
Verification
Ballot Data Flow


Alice
Bridget
encryption
Encrypted Votes
anonymization
decryption
Tally
Registration Database
Results
Verification
Ballot Data Flow

The Need for Simple

The Need for Simple

- Too complicated = disenfranchisement.
  voter experience needs to be almost as simple as it is today

The Need for Simple

- Too complicated = disenfranchisement.
  voter experience needs to be almost as simple as it is today
- Intuitive enough for officials to adopt

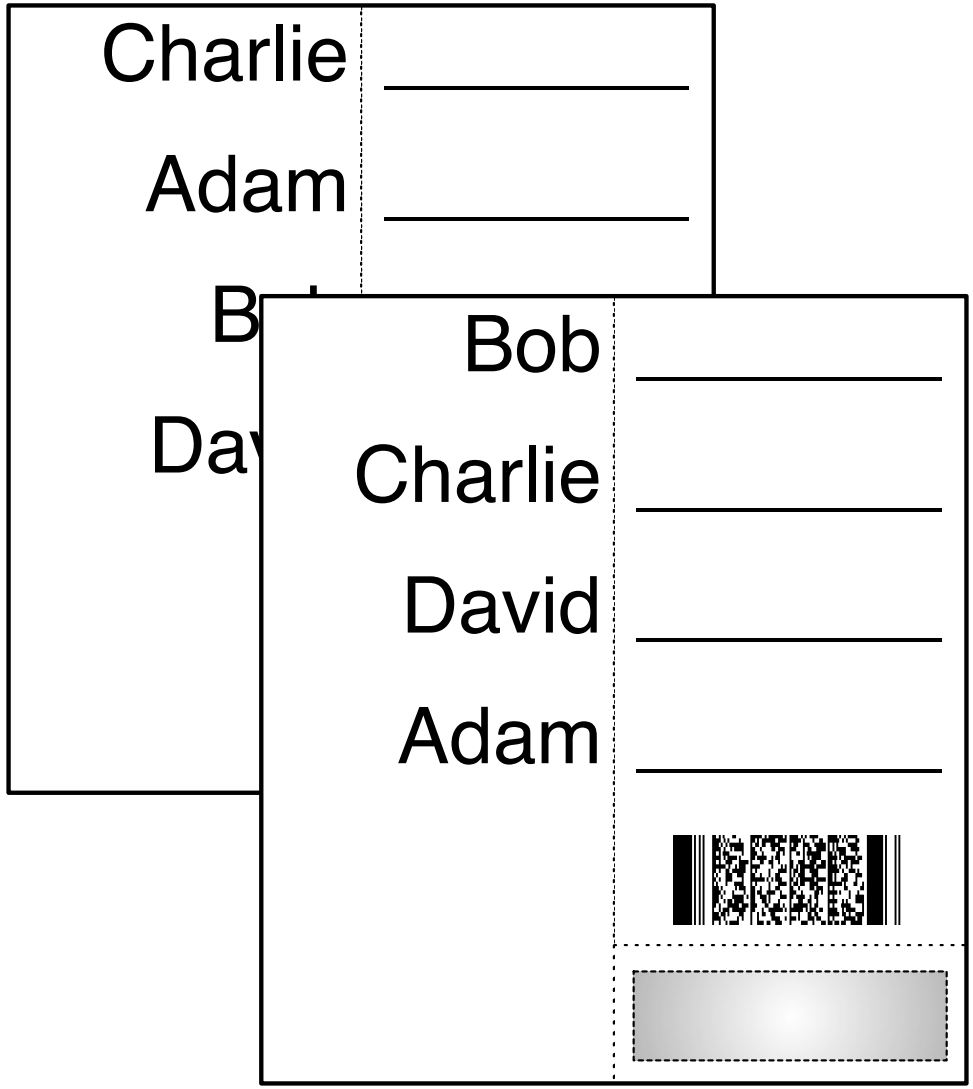
The Need for Simple

- Too complicated = disenfranchisement.
  voter experience needs to be almost as simple as it is today
- Intuitive enough for officials to adopt
- But... let's not expect everyone to understand everything.

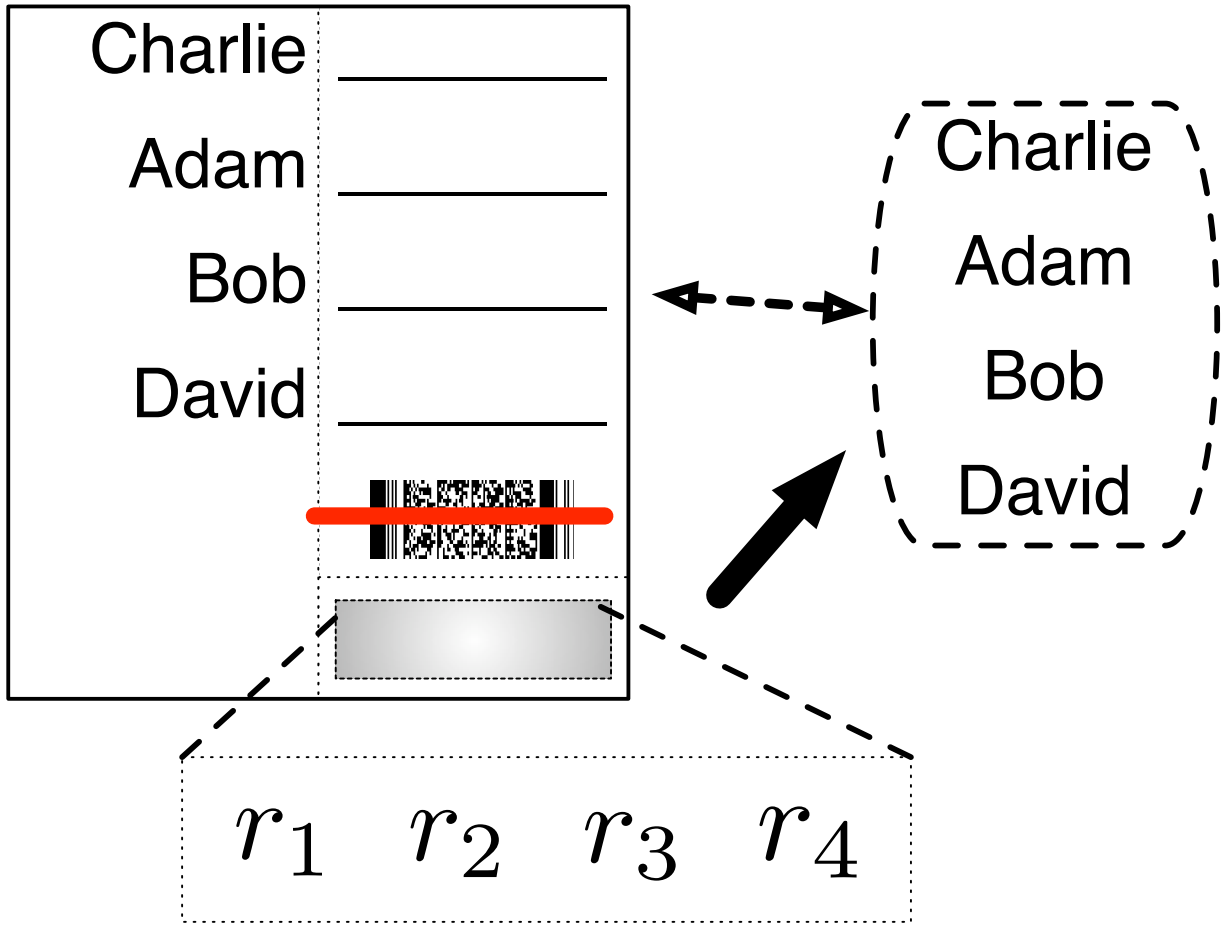
Continuing the Simplicity Trend

- Chaum's Punchscan
- Ryan's Prêt-à-Voter
- Benaloh's "simple cryptographic voting"

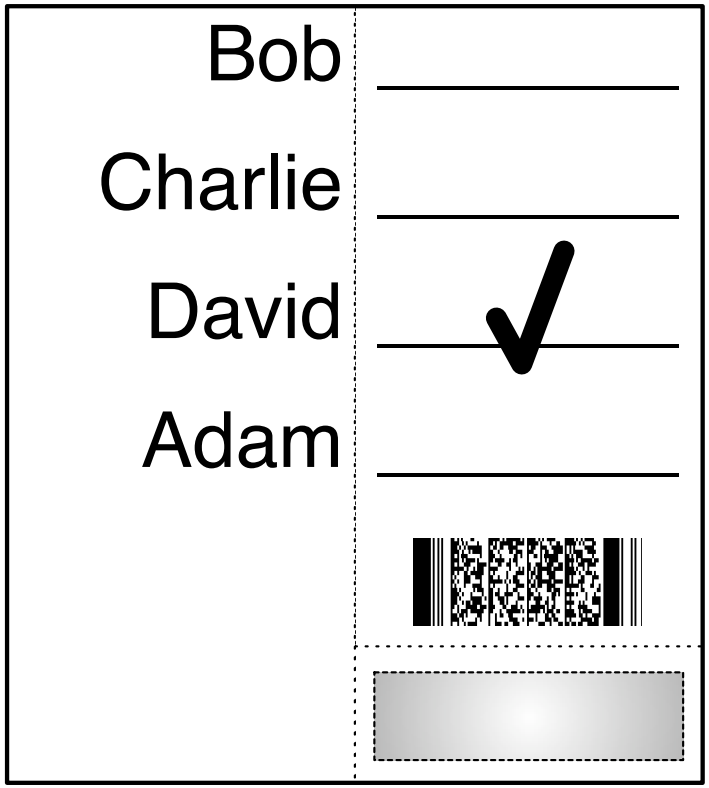
Scratch-and-Vote Experience



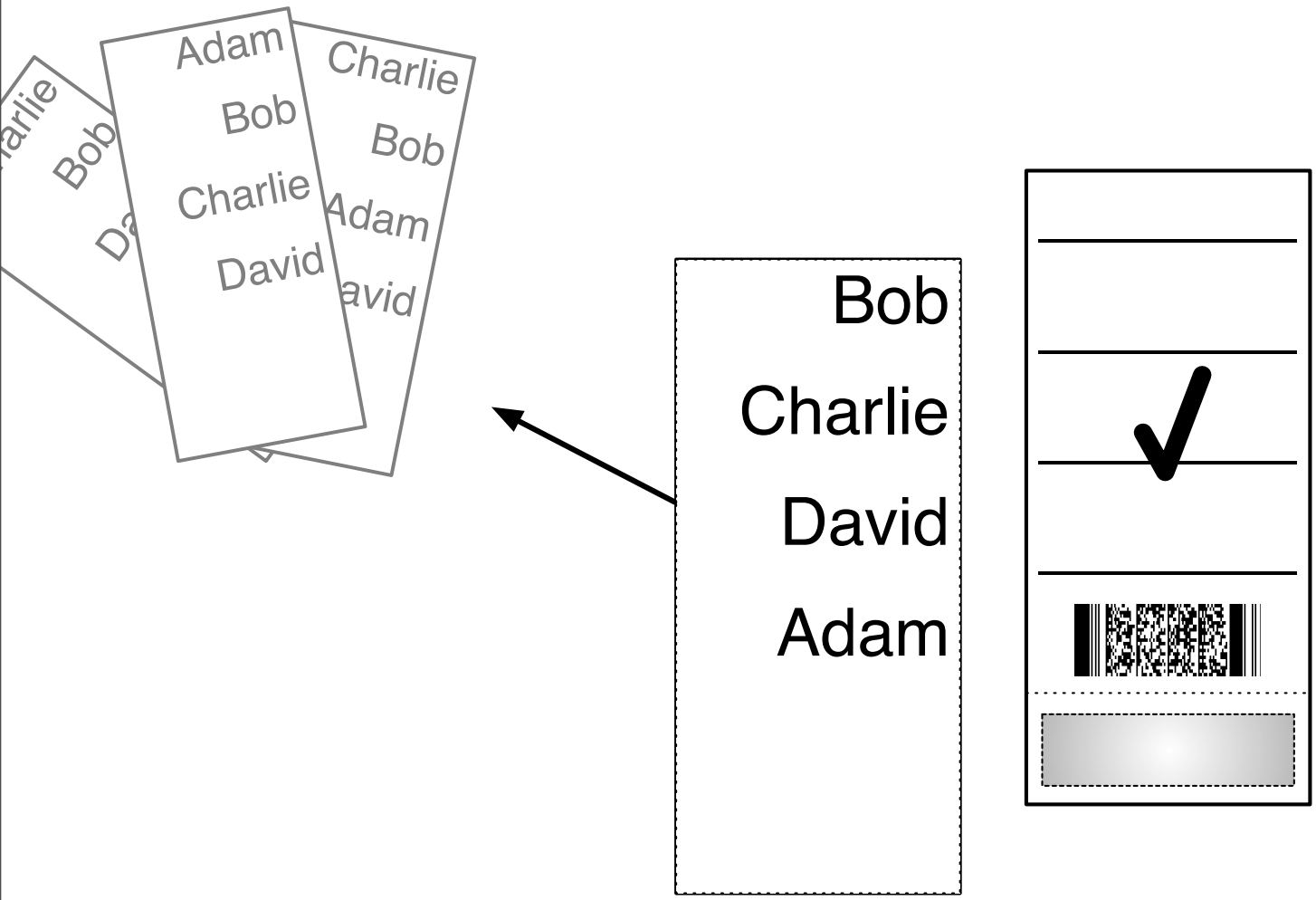
1. Receive two ballots.



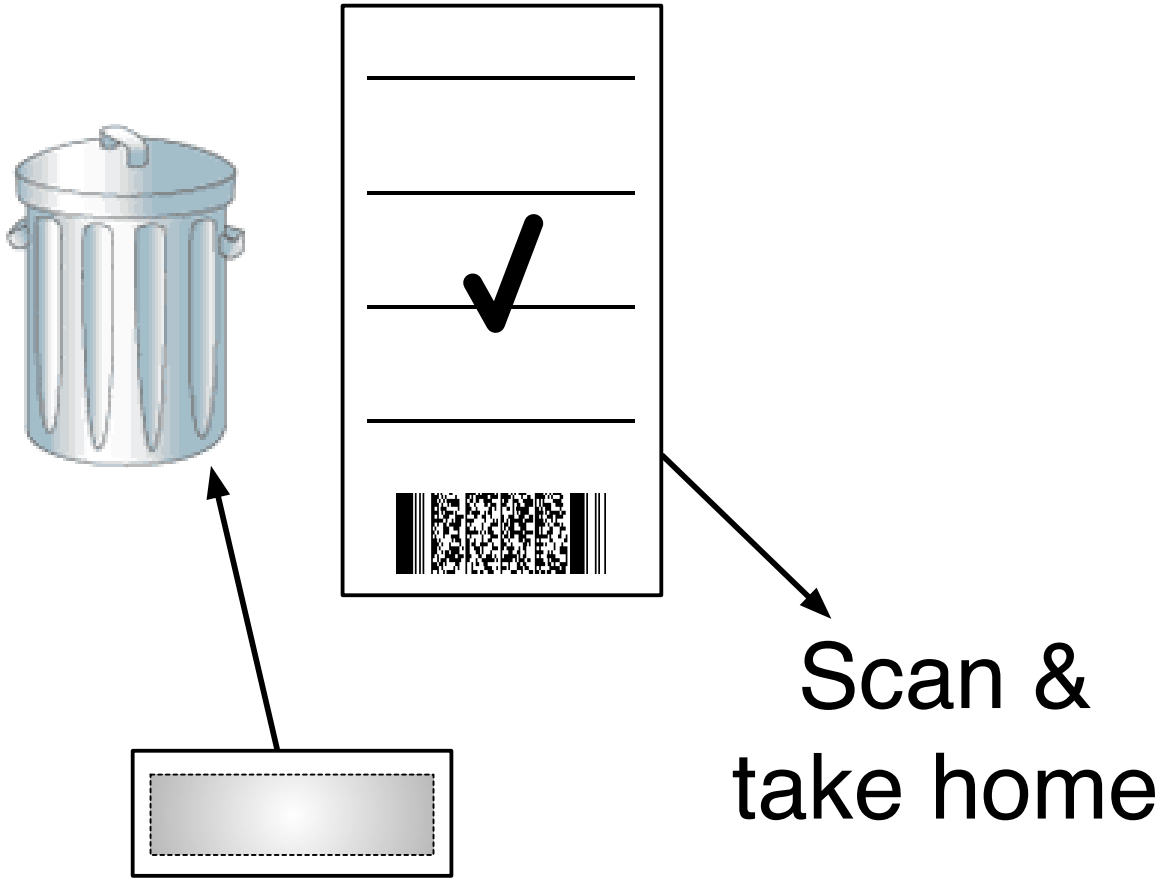
2. Choose one randomly for auditing by scratch-off.



3. Vote.

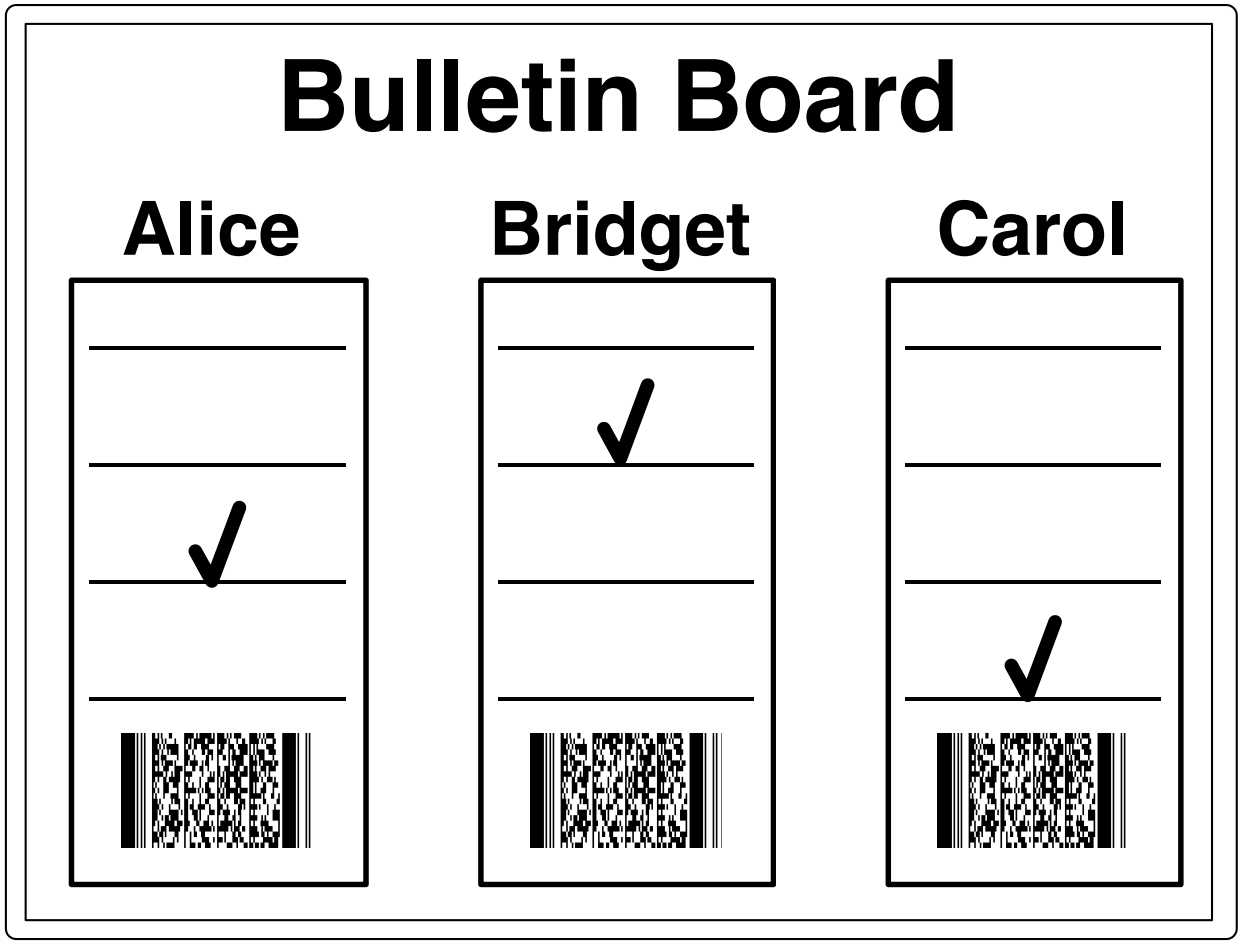


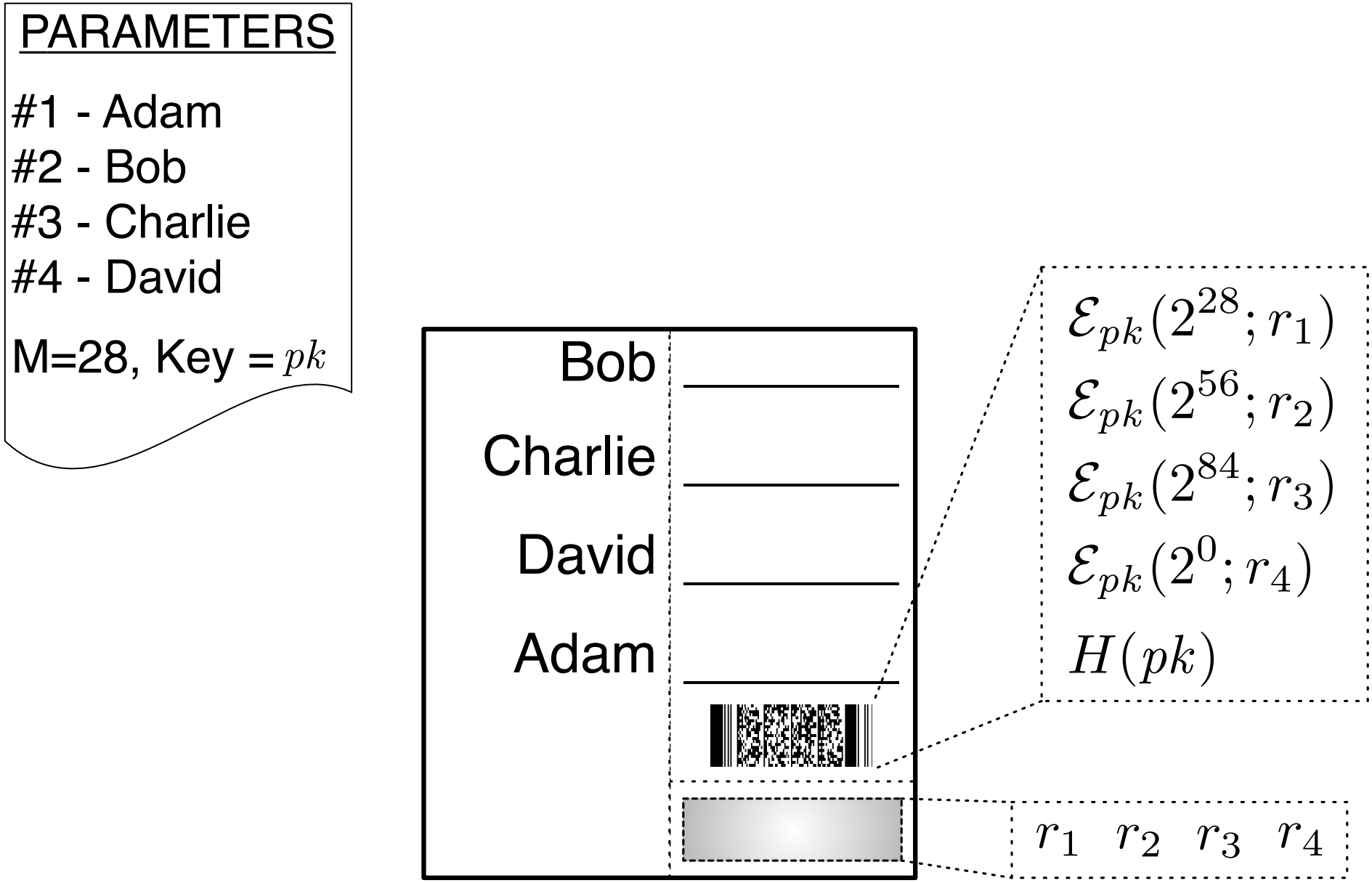
4. Tear & Discard left half of ballot.



5. Tear & Discard scratch-off.

Tallying


Bulletin Board
Alice
Bridget
Carol


PARAMETERS
#1 - Adam
#2 - Bob
#3 - Charlie
#4 - David
M=28, Key = pk
Bob
Charlie
David
Adam
$\mathcal{E}_{pk}(2^{28}; r_1)$
$\mathcal{E}_{pk}(2^{56}; r_2)$
$\mathcal{E}_{pk}(2^{84}; r_3)$
$\mathcal{E}_{pk}(2^{0}; r_4)$
$H(pk)$
r_1 r_2 r_3 r_4

Homomorphic Tallying

0001	0000	0000	0000

→ Vote for Adam

0000	0001	0000	0000

→ Vote for Bob

0000	0000	0001	0000

→ Vote for Charlie

0000	0000	0000	0001

→ Vote for David

0004	0001	0008	0002

→ **Sample Tally**

[B+2001, P1999]

Proof of Ballot (NIZK)

Proof of Ballot (NIZK)

- Malicious Voter submits: `Enc(1000)`

Proof of Ballot (NIZK)

- Malicious Voter submits: `Enc(1000)`
- in S&V, ciphertexts are picked ahead of time

Proof of Ballot (NIZK)

- Malicious Voter submits: `Enc(1000)`
- in S&V, ciphertexts are picked ahead of time
- but... what if election officials collude with a voter to throw the election with a bad ballot?

Proof of Ballot (NIZK)

- Malicious Voter submits: `Enc(1000)`
- in S&V, ciphertexts are picked ahead of time
- but... what if election officials collude with a voter to throw the election with a bad ballot?
- election officials must prepare proofs of correct ballot form ahead of time, on bulletin board (~80K per full ballot).

Practical Considerations

<u>5 questions, 5 options per question.</u>

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

Limitations

- *Write-in Votes*: not supported
- *Take-Home Receipt*: not currently legal

Scratch & Vote

- *Personal Verification*: scratch and verify
- *Open-Audit*: anyone can verify the tally
- *Incoercible*: voting booth & encryption
- *Simple*: common & cheap tech, process is close to current voting.

Questions?