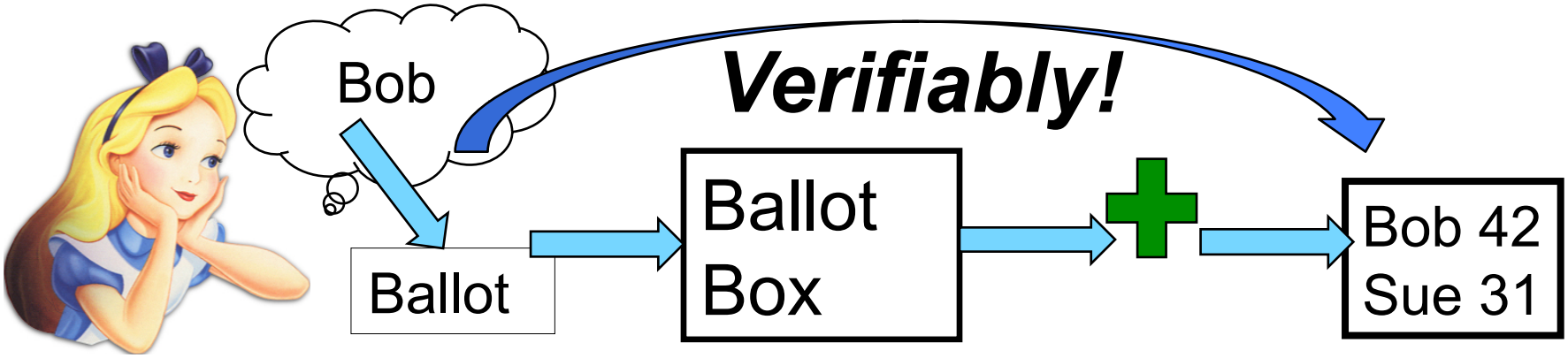


Perspectives on "End-to-End" Voting Systems

Ronald L. Rivest

MIT CSAIL

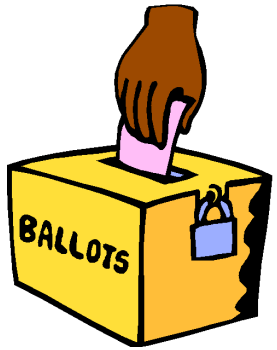
NIST E2E Workshop

George Washington University

October 13, 2009

Change happens!

- Greeks: pottery shards
- Public voting (early U.S.)
- Paper ballots preprinted by parties
- Australian paper ballots (mark choice)
- Lever machines
- Punch cards
- Optical scan
- DRE (Touch-screen)
- DRE + VVPAT (paper audit trail)
- Vote by mail (absentee voting)
- …



Change happens!

- Diffie and Hellman, 1976:
  - "We stand today at the brink of a revolution in cryptography."
- Today, we see evidence of a similar revolution in voting systems:

  Voting systems for which the statements:

  ``Trust me" and

  ``The hardware and software have been thoroughly tested!"

  are no longer acceptable justifications of an election outcome!

2000 Bush v. Gore

- A real 9.0 ``earthquake''
- Put spotlight on U.S. voting systems, which clearly needed improvement!
- Help America Vote Act (HAVA) 2002:
  - Threw money at the problem
  - Provided a means for better standards to (eventually) be devised
  - Created EAC (Election Assistance Commission)

Academics get (more) involved, too!

- 2001 CalTech/MIT Voting Technology Project
- 2005 NSF Funds ``ACCURATE" (A Center for Correct, Usable, Reliable, Auditable and Transparent Elections)

New conferences

- WOTE (Workshop on Trustworthy Elections) and EVT (Electronic Voting Technology) conference series start:
  - 2001: WOTE'01 (Bodega Bay)
  - 2004: DIMACS Workshop on Electronic Voting (WOTE II; Princeton)
  - 2005: FEE (Frontiers in Electronic Elections; Milan)
  - 2006: WOTE'06 (Cambridge UK)
  - 2007: WOTE'07 (Ottawa)
  - 2007: EVT'07 (Boston)
  - 2008: FEV (Frontiers of Electronic Voting; Dagstuhl)
  - 2008: WOTE'08 (Leuven, Belgium)
  - 2008: EVT'08 (San Jose)
  - 2009: EVT'09/WOTE'09 (Montreal)

New idea bubbles up: E2E

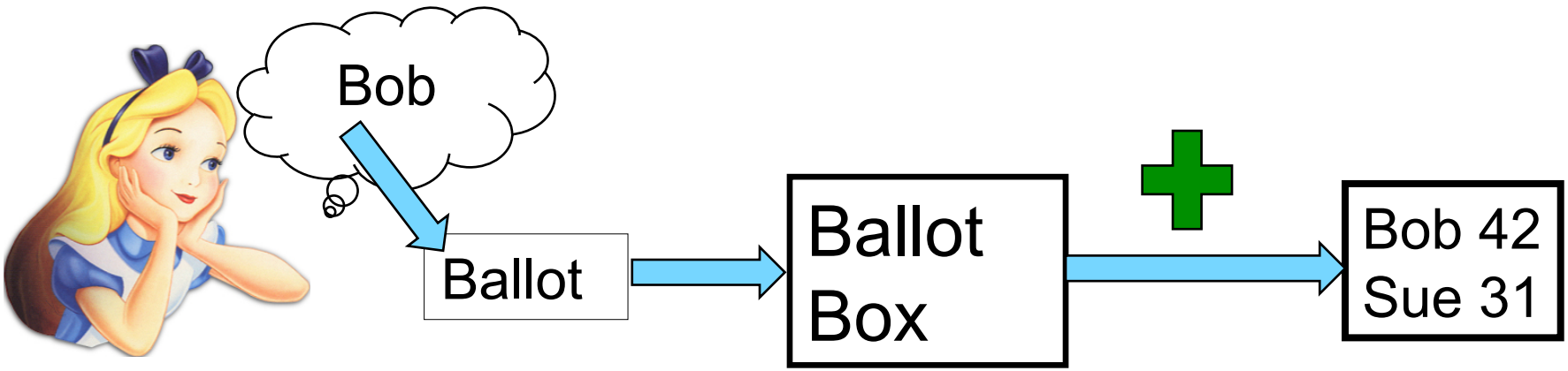
- A number of researchers proposed (at nearly same time, not necessarily independently) ideas for achieving higher assurance of election integrity, without having to trust hardware, software, election officials, and without violating voter privacy:
  - Chaum ('04 IEEE Sec/Privacy: visual crypto based)
  - Neff ('04: Vote Here)
  - Ryan ('04: Pret A Voter)
- Since then, field has blossomed… (Punchscan, Scratch-and-Vote, ThreeBallot, Scantegrity, Twin, Helios, … schemes without names …)

It's all about *verification!*

- Don't just check the equipment – *verify each election outcome!*

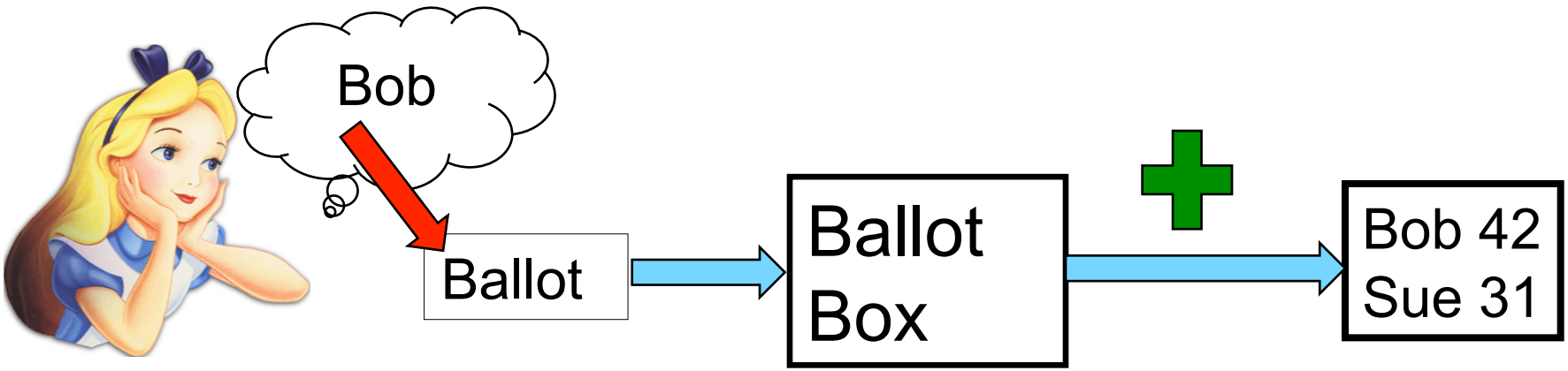
Voting Steps

- *recorded as intended*
- *cast (and collected) as recorded*
- *counted as cast*



Verifiable Voting Steps

- Verifiably *recorded as intended* (by voter)
- *cast (and collected) as recorded*
- *counted as cast*

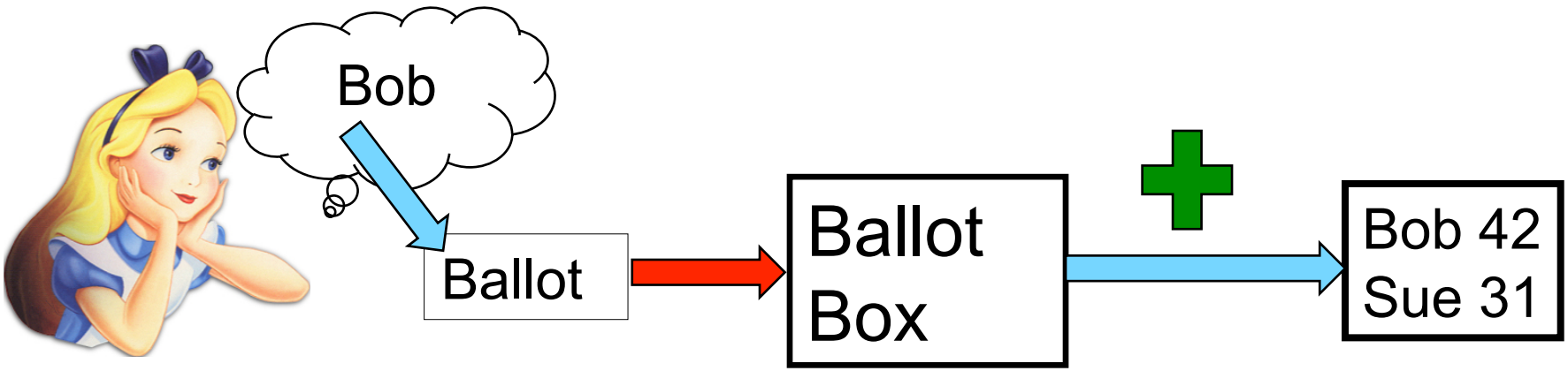


Verifiable Voting Steps

- Verifiably *recorded as intended*
- Verifiably *cast (and collected) as recorded*

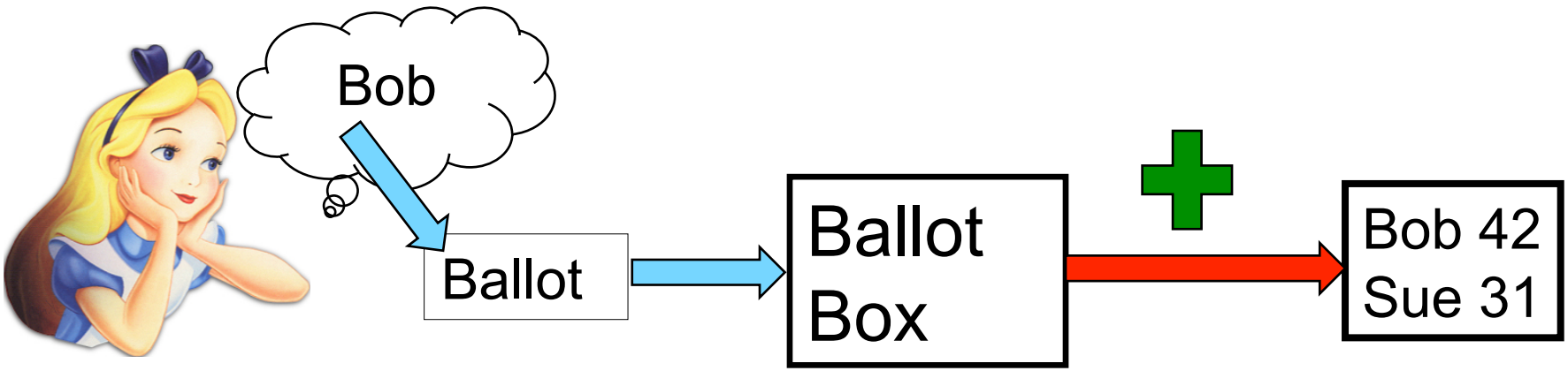
  (by voter)

- *counted as cast*



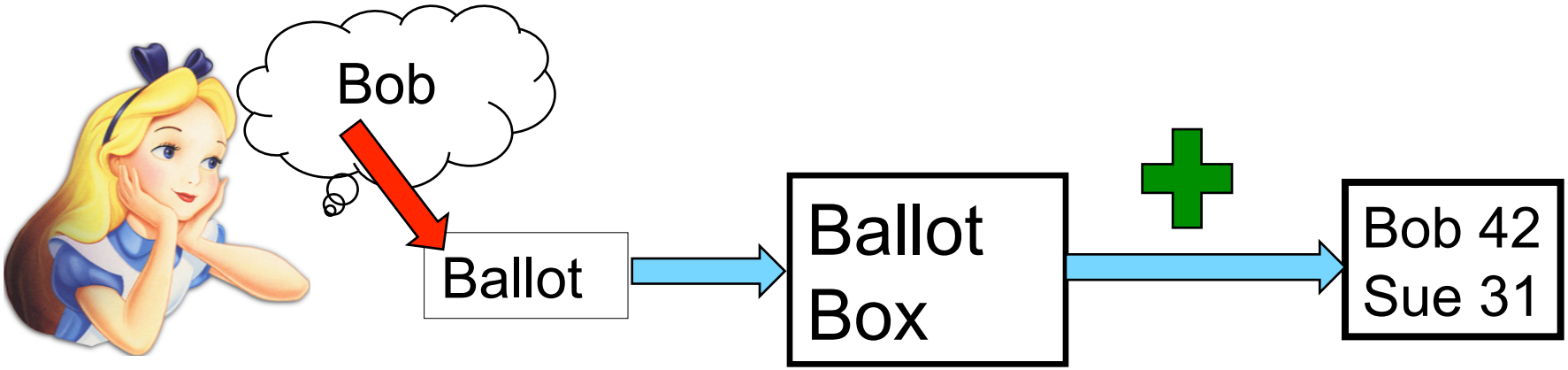
Verifiable Voting Steps

- Verifiably *recorded as intended*
- Verifiably *cast (and collected) as recorded*
- Verifiably *counted as cast* (by anyone)



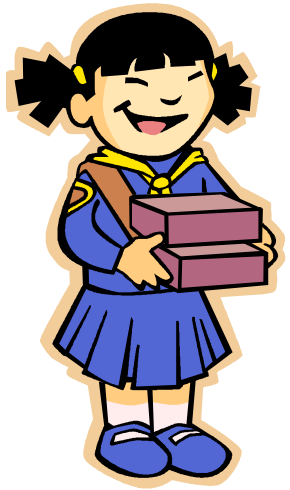
Verifiably Recorded as Intended?

- Only voter knows her intentions, and these should be kept private, so only she can verify the record of her vote.
- This is relatively easy with paper ballots (hand-marked or machine-marked)
- What about non-paper computer records?



Viewpoint on high-tech

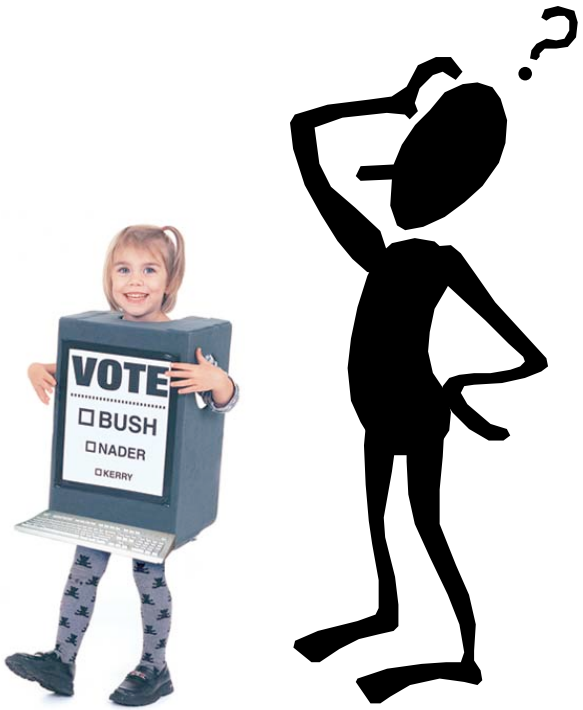
- *We should think of a computer (or other forms of "high tech") as a very fast and well-trained four-year old child.*
- The child may be very helpful (she is fast, and well-trained!) but may not always do the right thing (she's only four!).
- For something as important as an election, a ``grown-up'' should always check her work.



You just can’t

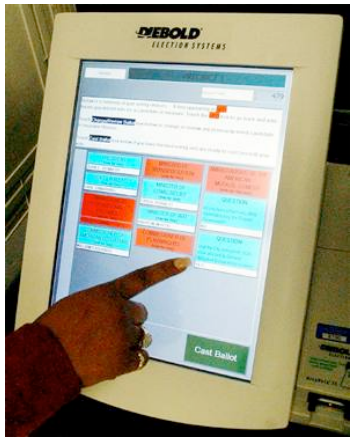
- do a ``logic and accuracy’’ test on a four-year old to ensure that she will do the right thing later!

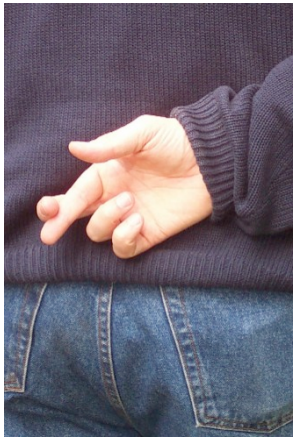
- design and/or certify a perfect four-year-old who always does the right thing!



Verifiably Recorded as Intended?

- What about non-paper computer records?
- Trusting a computer is rather like whispering in the ear of a four-year old, and hoping she'll record your vote correctly.





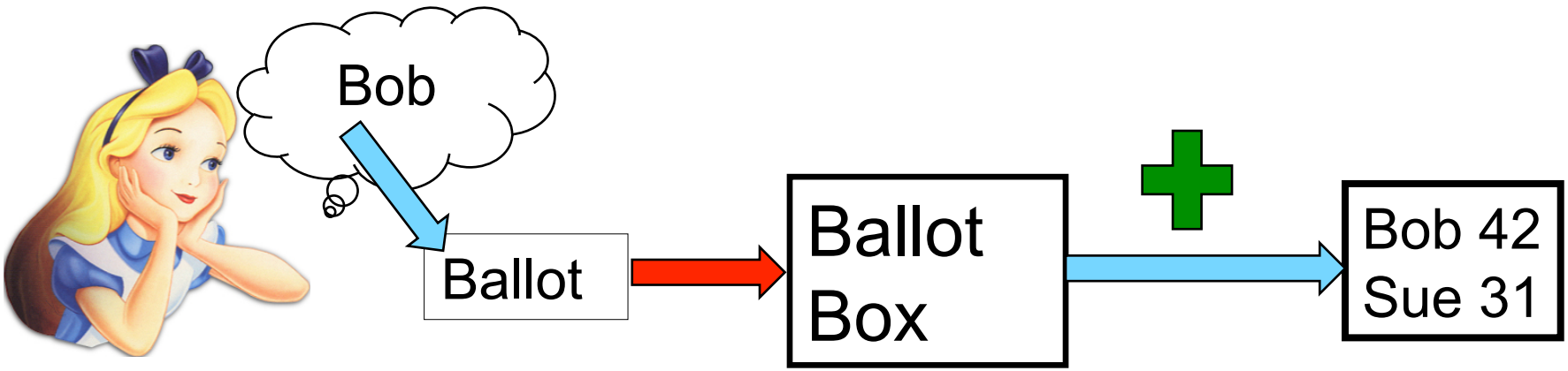
- Use paper ballots, or figure out how to verify that four-year-old is recording your vote correctly…

Verifiable Voting Steps

- Verifiably *recorded as intended*
- Verifiably *cast (and collected) as recorded*

  (by voter)

- *counted as cast*



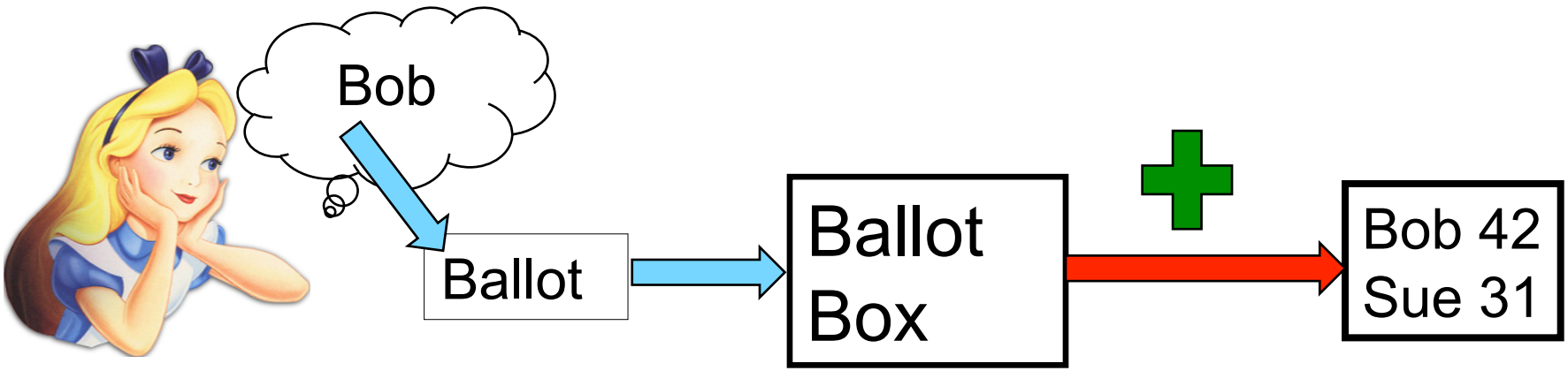

Where is my
VOTE?

Verifiably *cast (and collected) as recorded??*

- Collection of cast ballots needs to be *public*, and cast ballots need to be *identifiable*, so voter can find her ballot and check that it is correctly included.
- Most E2E proposals put cast ballot collection on a web site that voters may access.
- But, voter should not be able to *sell her vote!* Ballots should be *encrypted;* voter may be given ciphertext, as *receipt* (i.e., *encrypted receipt*).
- Recorded-as-intended verification also then needs to check enciphering (done by a fast four-year old!)…
- Now we have something new: *verifiable chain of custody!*

Verifiable Voting Steps

- Verifiably *recorded as intended*
- Verifiably *cast (and collected) as recorded*
- Verifiably *counted as cast* (by anyone)

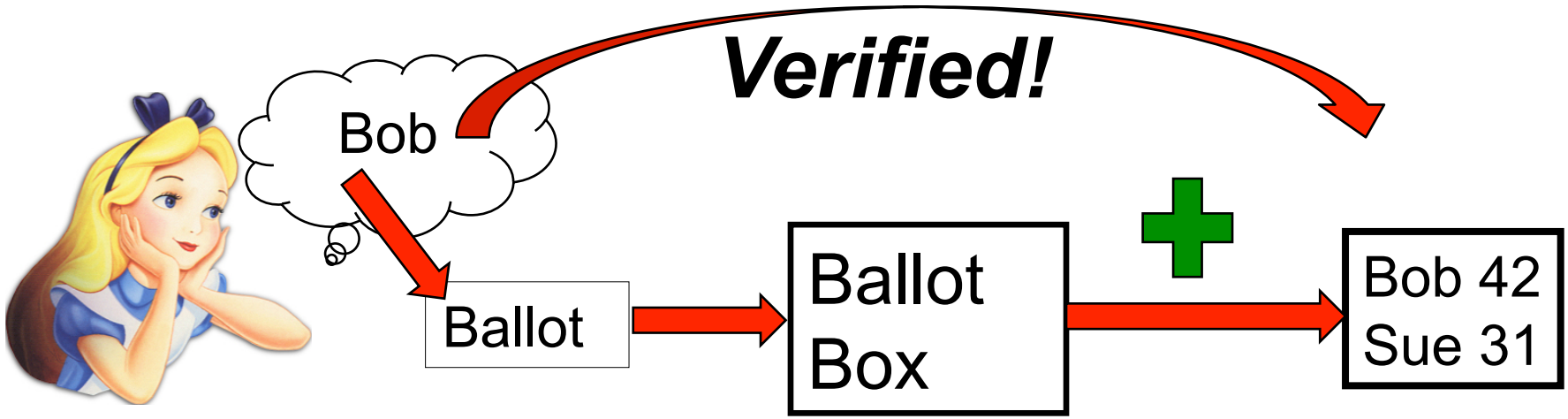


Verifiably *counted as cast ??*

- Given a collection of *encrypted* cast ballots, how can we produce a *verifiable* final result?
- This problem is well understood, and not as hard as it looks.
- You can decrypt collection first, as long as voter can't prove which plaintext corresponds to her ballot. This can be done using *mixnets*, which allow anyone to check correctness of decryption.
- Then, tallying plaintext ballots is easy.
- Other approaches also work.

Verified Voting Steps

- Verified: *recorded as intended* (by voter)
- Verified: *cast (and collected) as recorded* (")
- Verified: *counted as cast* (by anyone)



E2E is qualitatively new

- E2E voting systems provide greater assurance that the election outcome is correct than traditional systems (e.g. even opscan with post-election auditing).
- No need to trust ``four-year olds'' (or election officials) for integrity of election outcome (``four-year-old-independent'' = S.I.)
- There are many proposed variations on these ideas.

Some issues are unchanged

- Still need to control *who* may vote, and how often (ballot-box stuffing an issue, as with any voting scheme).

Tradeoffs

- E2E provides increased integrity of election outcome, at some cost in terms of
  - Support needed for new steps (e.g. verification steps), and for web site as public ``ballot box”
  - Usability
  - Transparency // complexity ??
  - Increased potential for voter privacy violations

Detection vs. Prevention

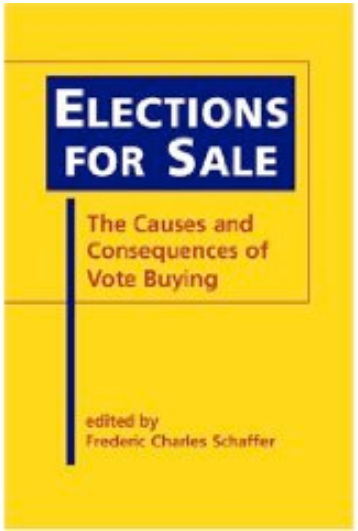
- Verification is only ``error detection'', not ``error prevention'' – you need to be able to deal with verification failures:
  - *Recording error*: spoil ballot | fire four-year-old
  - *Cast/collection error*: detect loss of ballots (not a new problem). Easy to fix if voter has (encrypted) balot copy. Watch out for mischievous voters!
  - *Tally error*: re-do tally
- (And, of course, make sure your election officials and ``four-year-olds'' are all well-trained, to minimize problems and protect privacy!)

Challenge – *paperless* E2E

- The purpose of E2E systems is primarily to improve election integrity through "end-to-end" verifiability.
- This doesn't preclude paper ballots. Indeed, paper ballots for E2E can be very attractive.
- However, some election officials would prefer election systems not involving paper (ballots).
- *Are there good <u>paperless</u> E2E voting systems?*

Challenge – *remote/mail* E2E

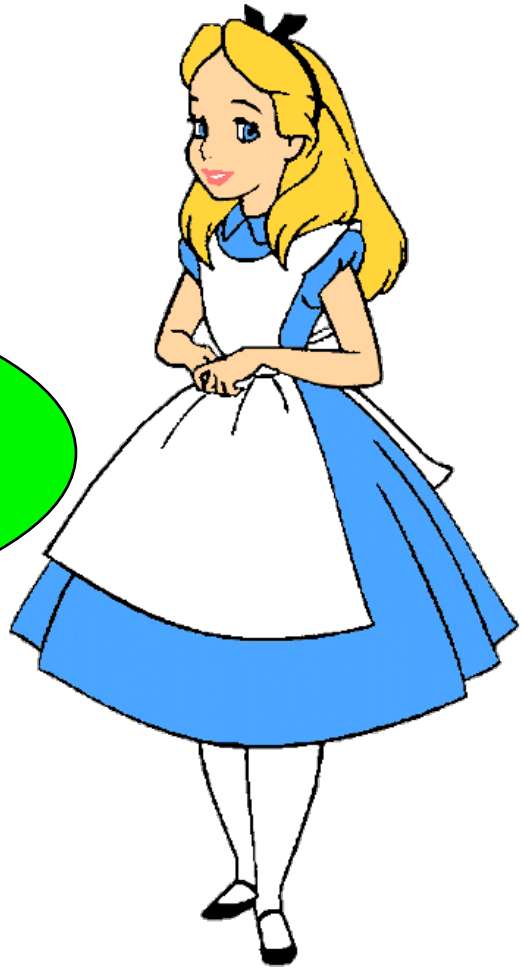
- *Are there good E2E voting systems for*
  - *Voting by mail?*
  - *Voting remotely by computer (non-poll-site)?*
- (Assuming that you are willing or forced to put voters in situations where they may be subject to coercion!)



Summary

- End-to-end voting systems provide a qualitatively new level of assurance for election outcomes: every step of the process, from voter's intent (in her head) to the final tally, is verifiable. Amazing!
- These systems are still evolving, but are starting to be usable (and used) in practice (Helios, Scantegrity,…)

Change is happening…



The (other) end
of this talk