
# Voting with Witness Voting:
## Qualified Reliance on Electronic Voting

WOTE '01

Tomales Bay, California, Aug 27-30, 2001.

Presentation by:

*Ed Gerck, Ph.D.*

*egerck@safevote.com*

*CEO & VP of Technology*

# Network Voting

Information about Safevote's network voting systems is available at:

- www.Safevote.com – technology
- www.MySafevote.com – election services
- info@safevote.com – contact

Provides several strong features, including:

- Receipt-freeness
- Universal verifiability
- Spoof prevention
- Free from coercion
- Free from vote selling

# Summary

This paper addresses the fundamental problem in public elections (the “vote gap” problem), which is that of tallying a ballot as seen and cast by a voter.

The significant aspect is that in order to preserve election integrity, no one should be allowed to prove what ballot was cast by a voter – not even the voter. The system must be designed to allow the voter to cast any ballot within a possible selection set.

DREs (direct recording electronic voting machines) are used to exemplify a method called “witness voting” (W-V) that is 100% digital and can be used to prove, with an error margin as close to zero as desired, that the ballot seen and cast by a voter using a DRE is the ballot that will be tallied. The W-V method does not need to change the DRE, does not use paper ballots and can be applied to network voting.

The W-V method also leads to methods called “real-time auditing” and "dynamic certification,” which can be applied to “black box” voting machines, so that at the end of an election one can objectively grade each election machine and decommission those machines that do not conform with what can become well-defined performance standards of accuracy and reliability. W-V also includes fault-prevention methods.

# Outcome Uncertainty

The outcome uncertainty of a voting system can be seen as accuracy and reliability problems in counting votes.

Lack of accuracy or reliability introduces two different types of errors:

- accuracy affects the spread of one event, for example whether a vote that was selected **to be** cast by a voter can be counted or not from a ballot;
- reliability affects a number of events in time and/or space, for example, count differences when repeatedly reading votes from the same stack of ballots.

# DRE – an expensive con machine?

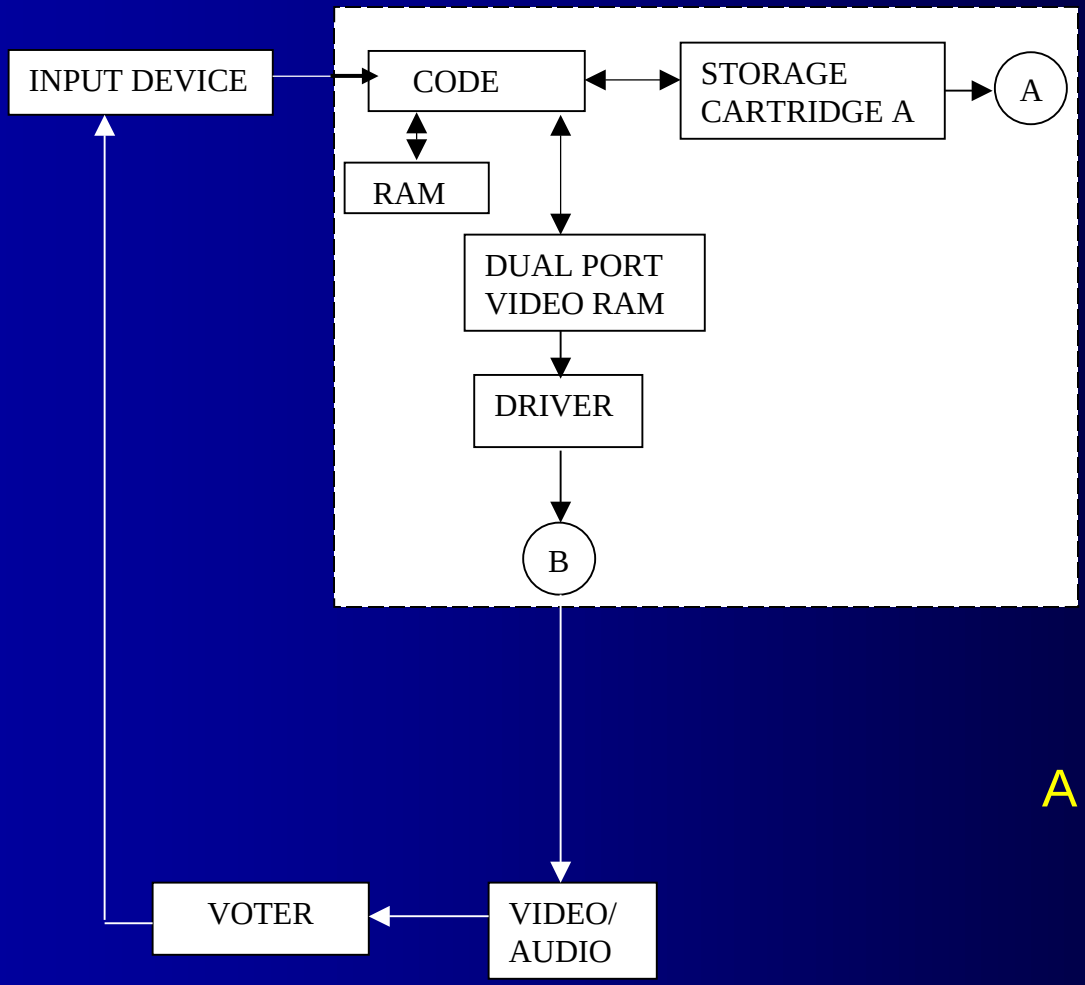
- DREs (direct recording electronic voting machines) are costly.
- There is no clear reason to trust a DRE vote count.
- DREs fail to prove that the vote stored in the machine is really what the voter saw and confirmed on the screen.
- DREs may behave as ideal "con machines" for voters.
- A DRE has no witness to its acts but itself.
- Open source software does not guarantee accuracy and reliability – bugs, fraud, virus, Trojan horses and faults can still influence the outcome, without possibility of detection.

# DRE – an expensive con machine?

- *"The fact that the voter can see his or her choices on a display, or even receives a printout of the choices made, does not prove that those were the choices actually recorded in the machine to be summarized for generating the results of the election."* [Roy G. Saltman, NBS, SP 500-158, August 1988]

- *"Electronic balloting systems without individual print-outs for examination by the voters, do not provide a wholly independent audit trail (despite manufacturer claims to the contrary)."* [Testimony by Rebecca Mercuri, U.S. HR Committee on Science Subcommittee on Environment, Technology, & Standards, Tuesday, May 22, 2001]

# Typical DRE design

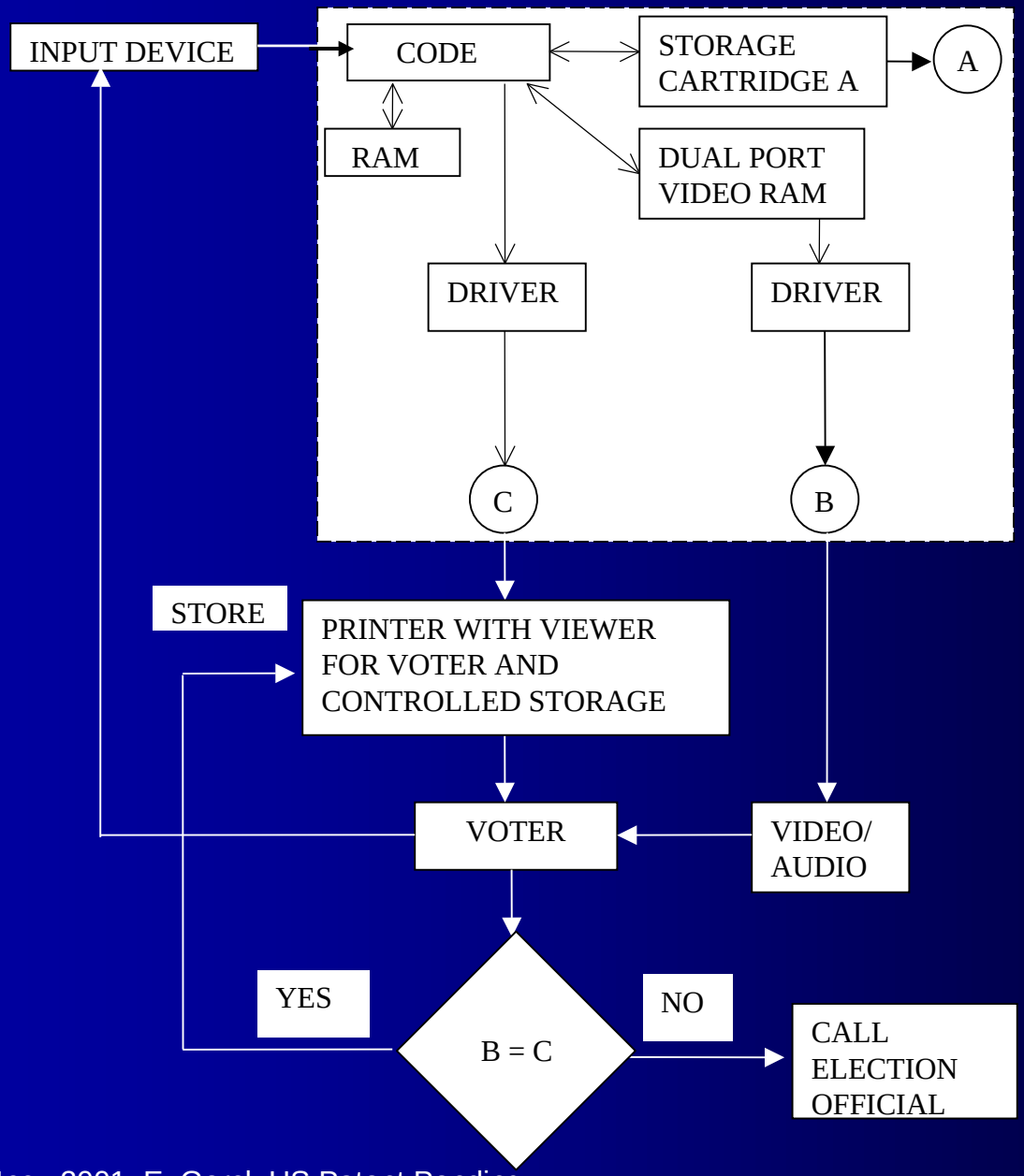



A < > B

# DRE – an expensive con machine?

- DRE machines with touch screens have been around for more than 10 years in the U.S.
- DRE machines have only 9% of the market.
- Adding paper ballots to DREs may prevent fraud, not necessarily correct it.
- Voters must not be relied to spot problems in the equipment they used to vote – long ballots, tiredness, lack of time, ergonomics, queues and presumption of trust mitigate against effectiveness of user verification.
- Paper ballots have to be stored, controlled and counted, with known difficulties and high cost, which is the main problem DREs intended to solve.

# DRE design with added paper ballots




A < > B

A < > C

B < > C

Because of long ballots, tiredness, lack of time, ergonomics, queues and presumption of trust, voters cannot be relied upon to verify machine errors.

# DRE – What NOT to do

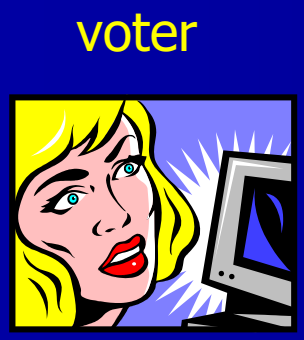
**Adding paper ballots does NOT solve the reliability problems of DREs.**

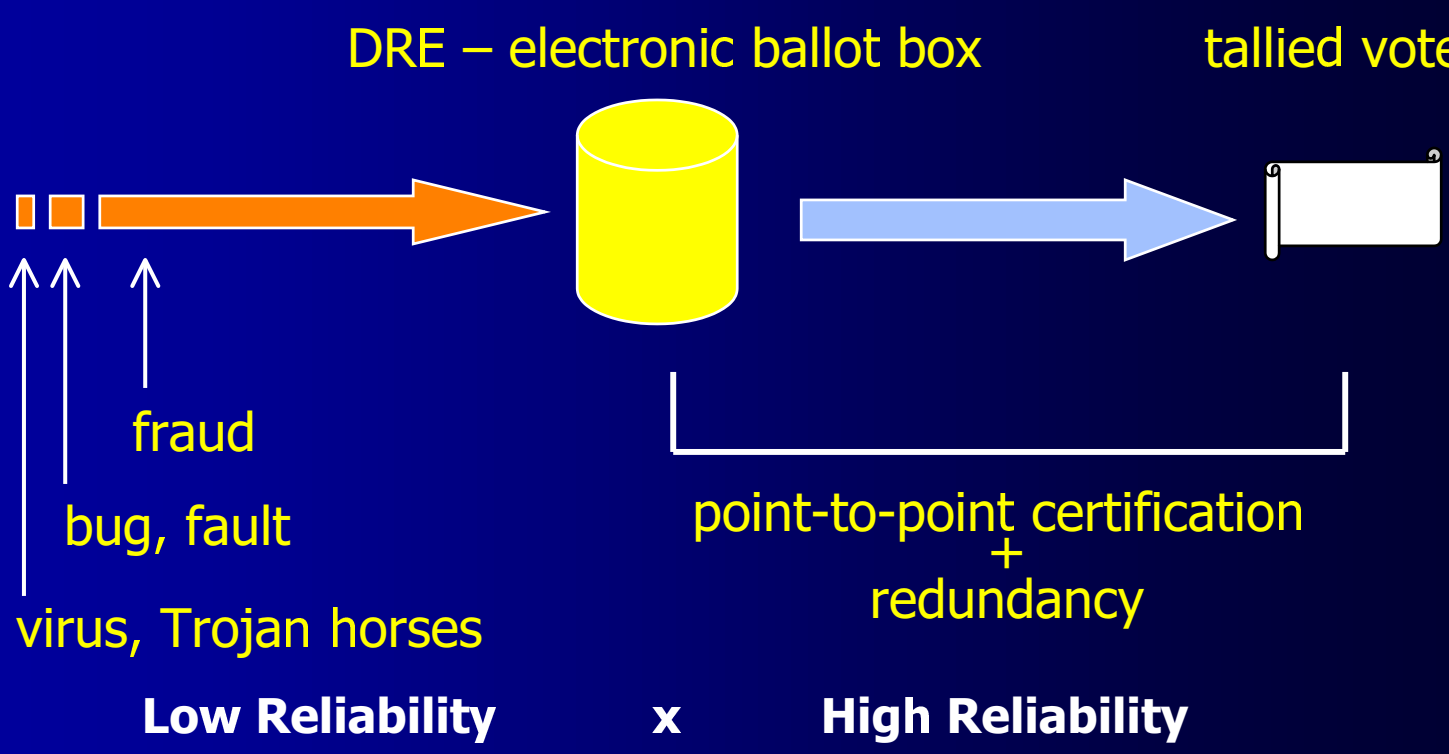
**DREs should NOT rely on paper ballots to solve paper ballot problems.**

**DREs should NOT rely on voters to spot equipment problems.**

**To motivate improved designs, certification requirements for DREs should NOT exclude the possibility of using closed source. Companies may want to use trade secrets to reduce cost, improve fault-tolerance, etc. Companies may need several years to reach positive ROI.**

# The Fundamental Problem of Electronic Voting






## Low Reliability

The "vote gap" problem: The voter cannot see her tallied vote, hence the voter cannot know whether her vote will be counted as selected.

# DRE – Solution Requirements

- Capture the “magical moment” – the primary information – when the voter confirms the choices seen on the screen.
- Create witnesses for the confirmed choices and possibly also for the ballot cast, which witnesses should be as simple, non-interpretive and independent as possible.
- Use witness and device redundancy to increase fault-tolerance.
- Do not interfere with the underlying voting process.
- Differences between witnesses are expected but must be resolvable.
- Use consensus protocols to provide a consistent view of the election outcome.
- A voting system's reliability should be measurable in real-time.
- An unreliable voting system should be terminated still during the election.

Mathematical Motivation:

If two witnesses are not 100% mutually dependent, the probability that both witnesses may fail at the same time is smaller than that of any single witness to fail.

# Optical Data Witness

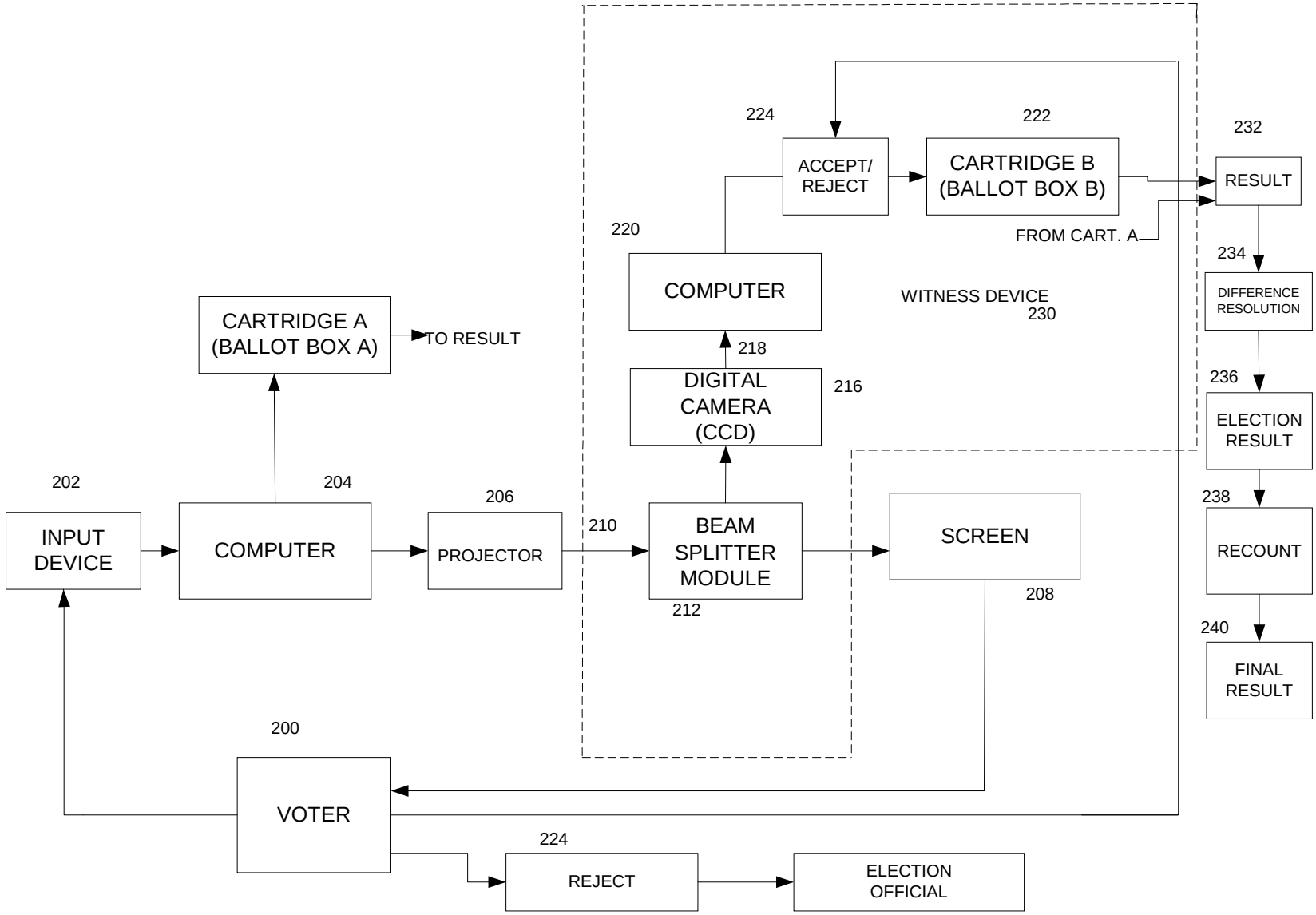



Fig. 2A

# Display Data Witness

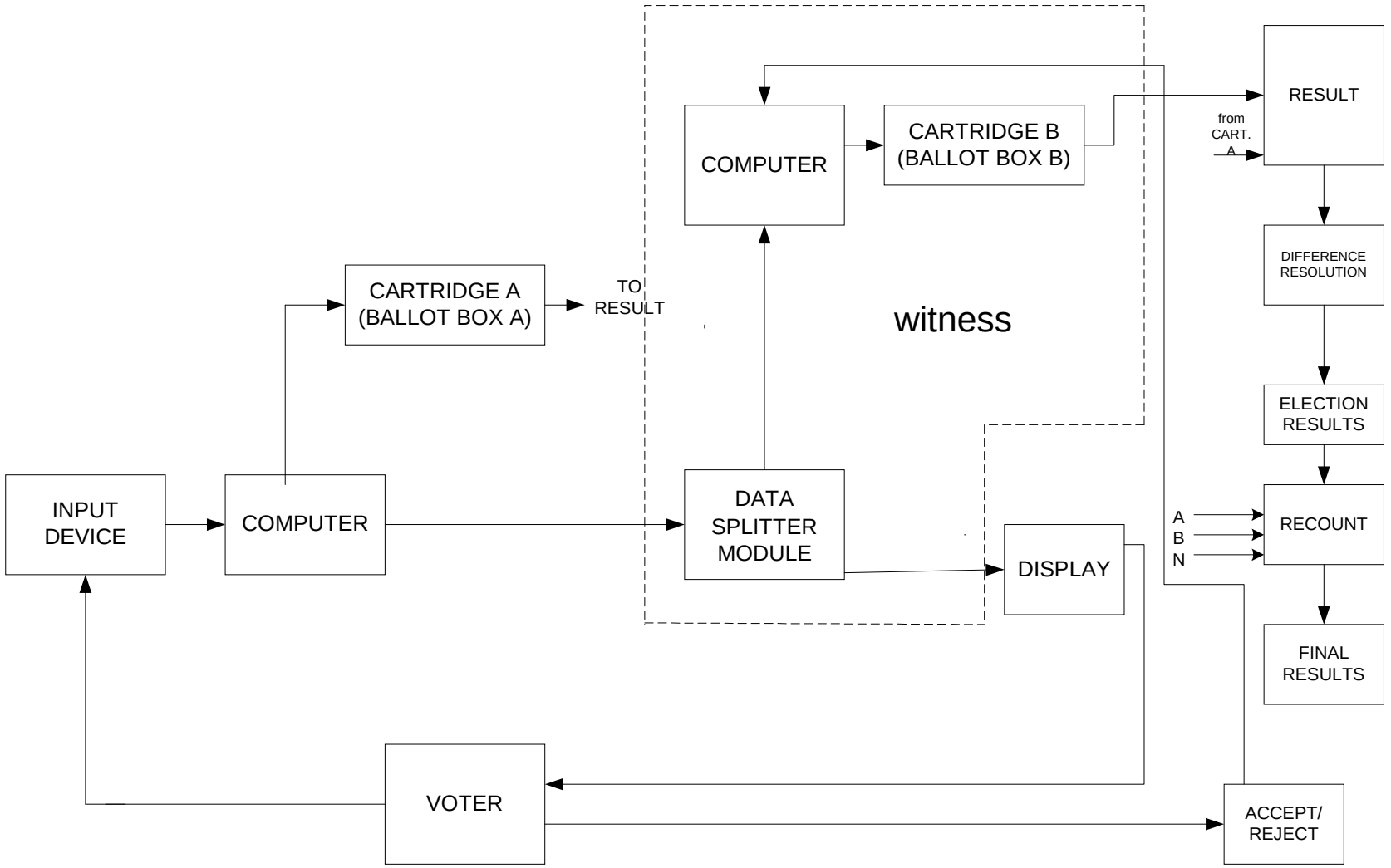



Fig. 2B

# Display Card Witness

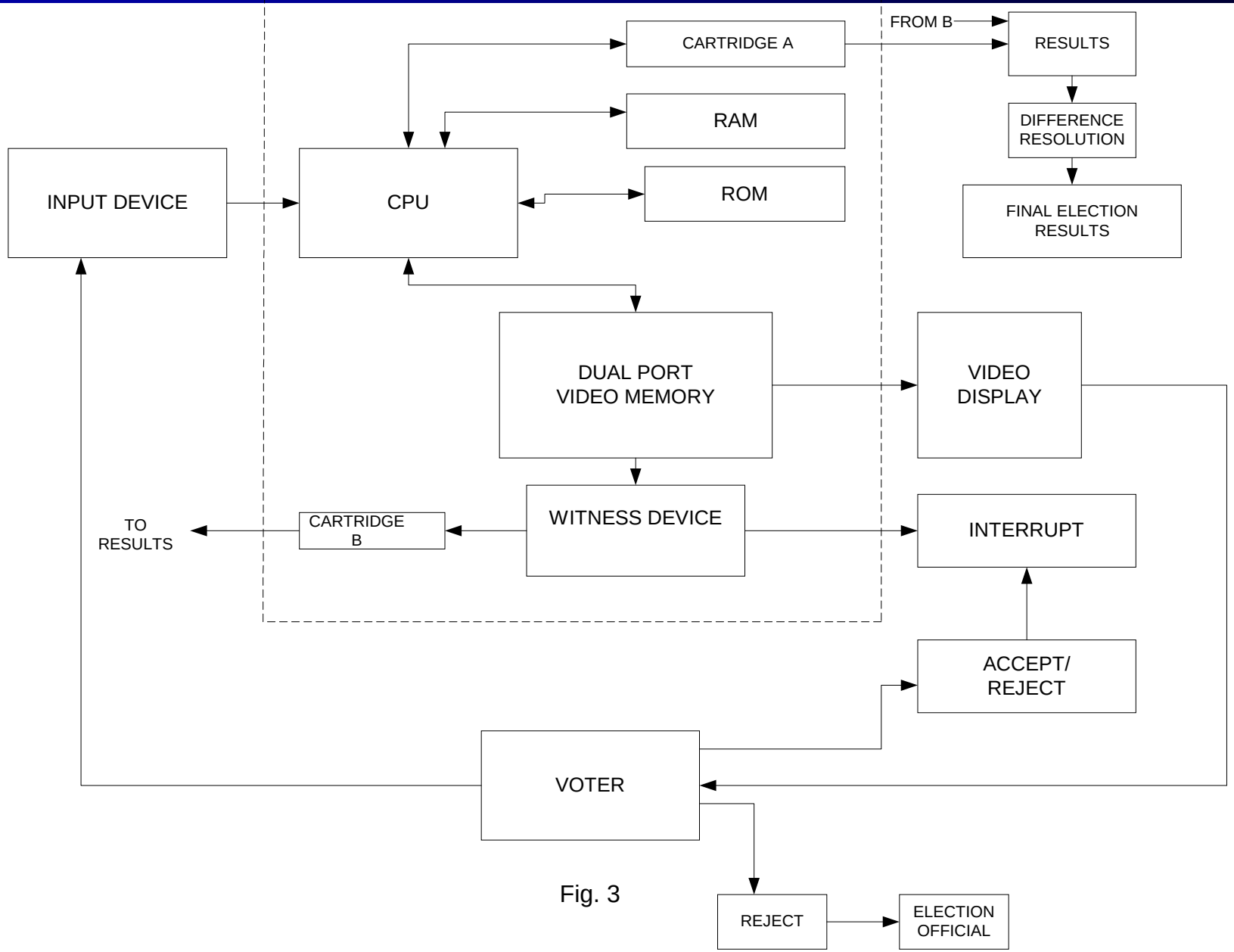
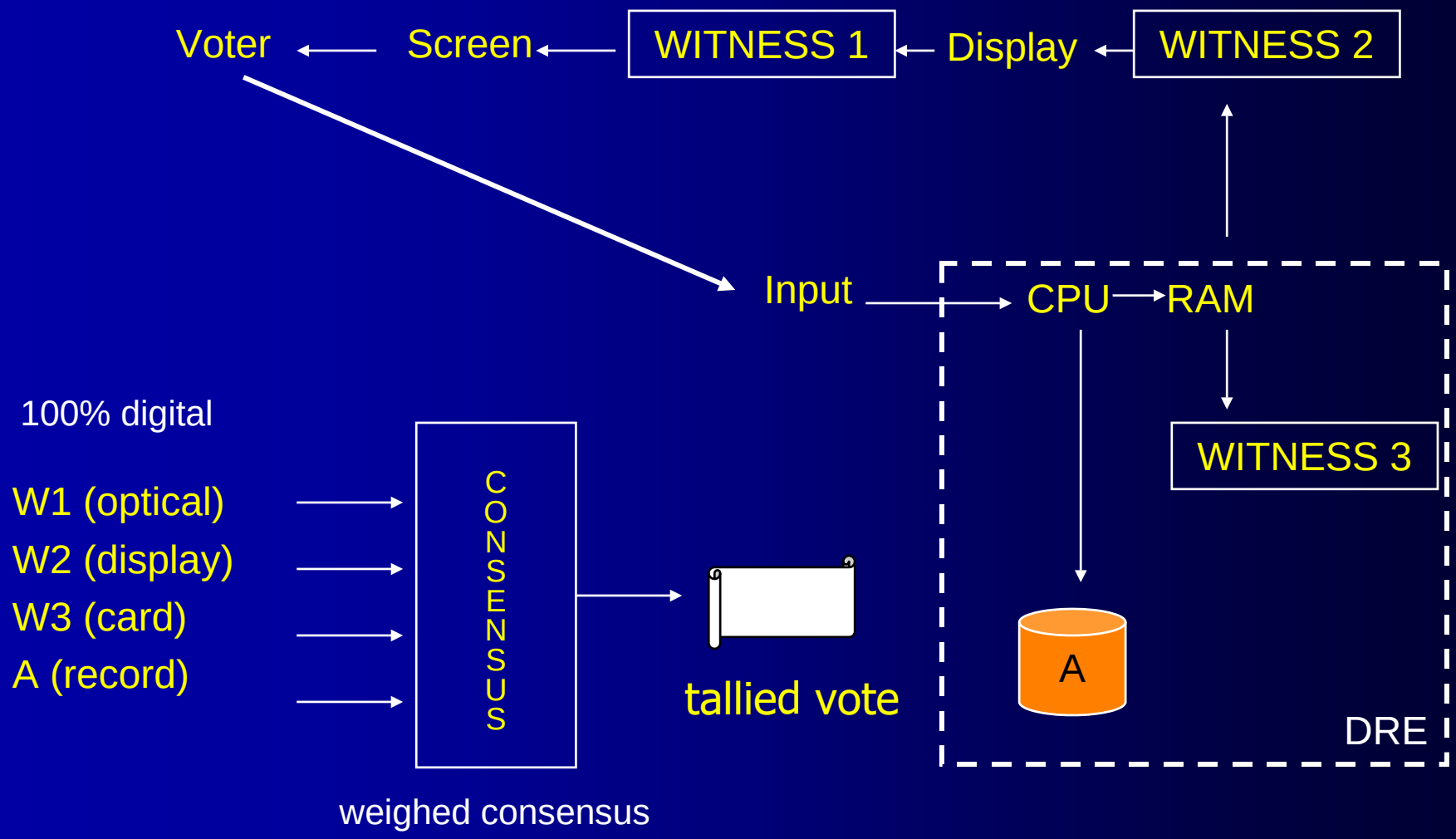



Fig. 3

# Optical, Display and Card Witnesses




Expected probability of compromise: W1 < W2 < W3 < A

# Consensus Protocols

Consensus protocols are used to increase consistency and are commonly implemented as voting protocols:

In distributed file systems, voting protocols may ensure the consistency of replicated objects by requiring all read and write requests to collect an appropriate quorum of replicas. Different quorums for read and write operations can be defined and different weights, including none, assigned to every replica.

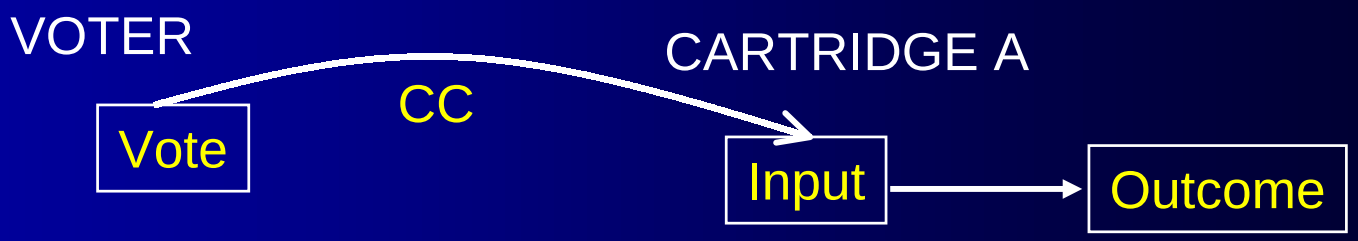
In distributed computing systems, computing modules can cooperate and maintain consistency based on a majority vote in order to tolerate faults among their members.

# Properties of Witness Voting Systems

- 100% digital
- reliability can be improved by increasing the number of independent witnesses
- fault-tolerance can be improved by adding redundancy to each witness
- consistency is obtained by consensus among the witnesses and the recorded vote
- witness devices can be simple and perform only simple tasks
- witness devices can use open source
- witness devices can be hardware-limited to be simple
- witness devices do not need interpretive functions
- witnesses can be data (image, sound), a fraction of data or just a signature
- witnesses can be stored in random order
- witnesses can be tallied automatically
- witness devices and witnesses can have different resiliency, availability and trust
- witness voting systems provide for auditing and verifiability
- witness voting systems can both prevent and correct errors

But ….what is the limit for reducing errors in voting?

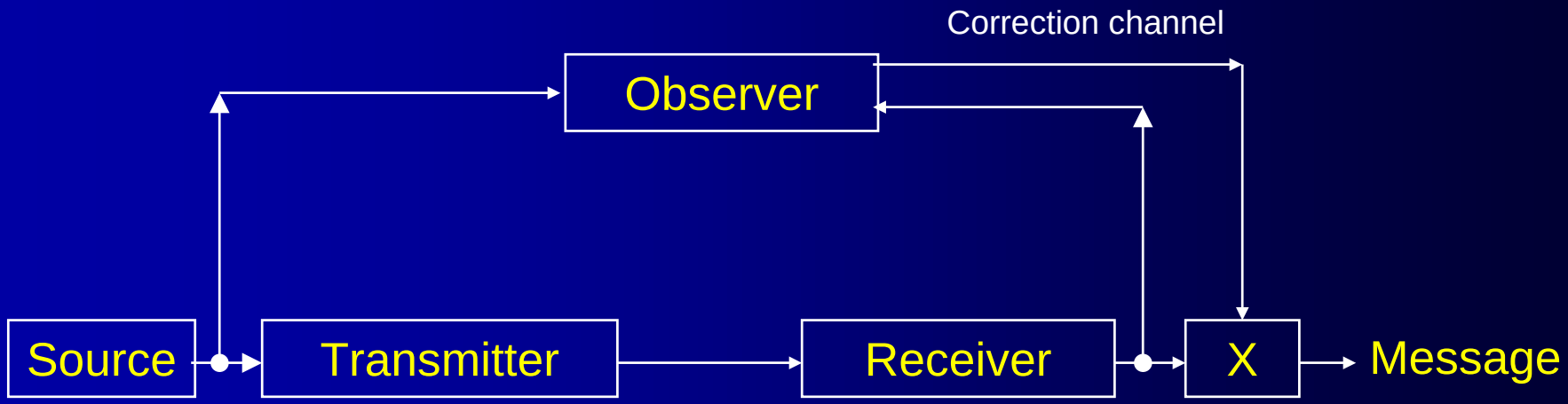
# Casting a Vote is Communication




- The Outcome of a voting system is calculated from Inputs collected from a set of voters according to a set of rules.
- For every Vote selected **to be** cast by a voter, a DRE (or other type of voting device) provides a communication channel (CC) connecting a Vote to an Input.
- The set of Inputs (I) should, ideally, be equal to the set of Votes (V) that were selected **to be** cast by each voter. The Outcome should thus, ideally, represent the Votes without errors.
- However, the communication channel CC is susceptible to disturbances, such as bugs, faults and attacks in several forms.
- These disturbances can add, modify or delete any number of inputs in the set I.
- The disturbances in the CC may have any statistics, losses and time dependency.
- The disturbances, including losses and time dependencies, can be modeled as noise.
- The differences between Votes and Inputs can be modeled as communication errors due to noise.

## What is the limit for reducing errors in communication?

# Reducing Communication Error

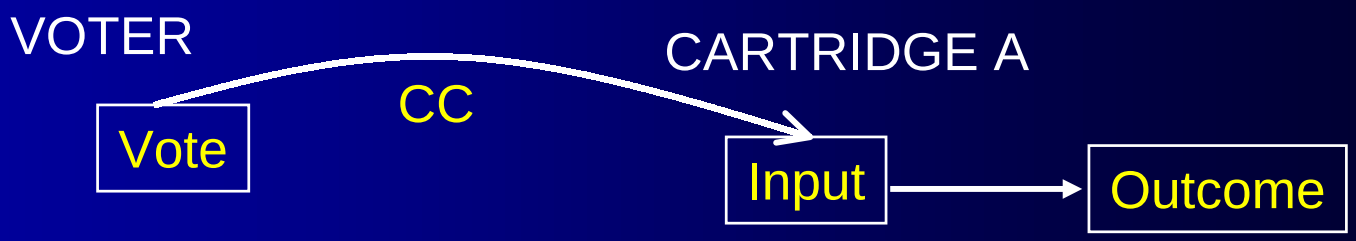



Tenth Theorem, Shannon:

"With the addition of a correction channel equal to or exceeding in capacity the amount of noise in the original channel, it is possible to so encode the correction data sent over this channel that all but an arbitrarily small fraction of the errors contributing to the noise are corrected. This is not possible if the capacity of the correction channel is less than the noise."

What is the limit for reducing errors in communication? Zero.

# Reducing Errors in Voting Systems




- A DRE can be seen as a communication channel (CC) between Votes (V) cast by voters and Inputs (I) stored in its cartridge. Faults, losses, bugs, frauds or attacks can be seen as noise.
- The limit to reduce errors in a communication system is zero. We can get arbitrarily close to zero, but not necessarily reach zero.
- This conclusion does not depend on any statistical assumption about the sources of noise nor about their possible dependencies or independencies.
- The only requirement is that we use a correction channel with capacity equal to or exceeding the amount of noise in the communication channel.
- The witness voting system functions as a correction channel in regard to the underlying voting system.

With an adequate witness voting system, all but an arbitrarily small fraction of the errors in the underlying voting system can be corrected.

# The Strength of Small Numbers

We  can randomly witness the underlying process, in samples.

We can accept a difference that makes no difference.

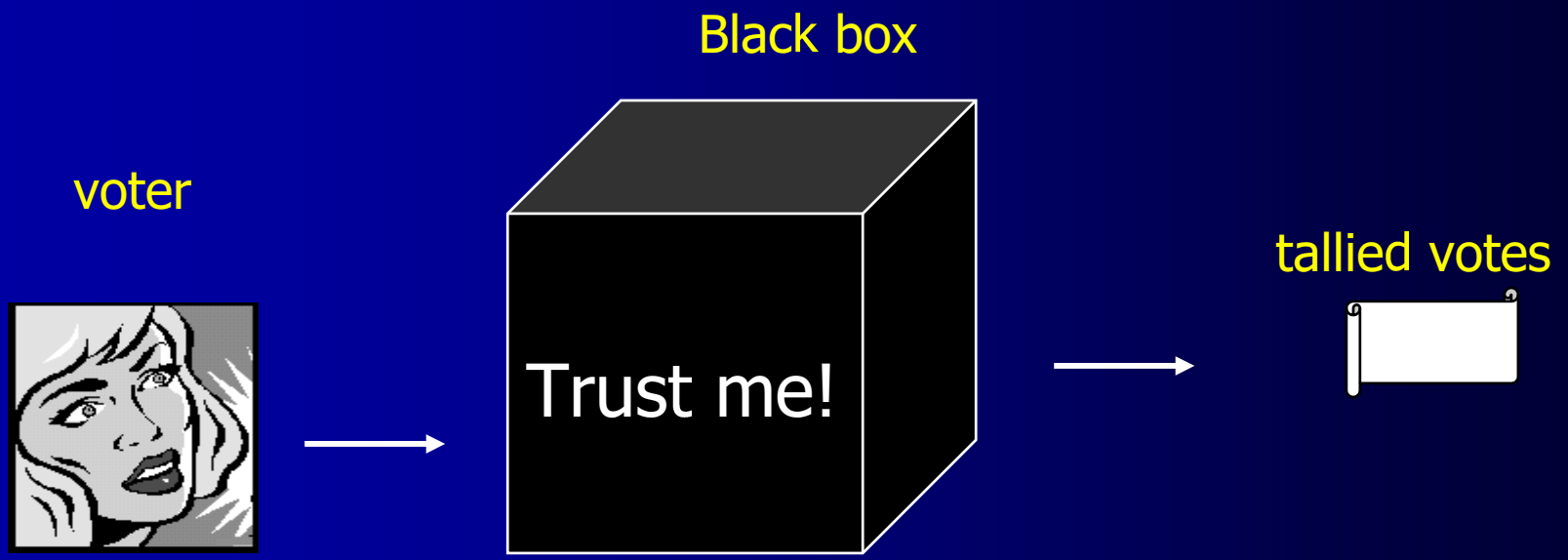
The witnesses can be distributed – network voting (Internet, dial-up).

The witness voting system can be distributed as well.

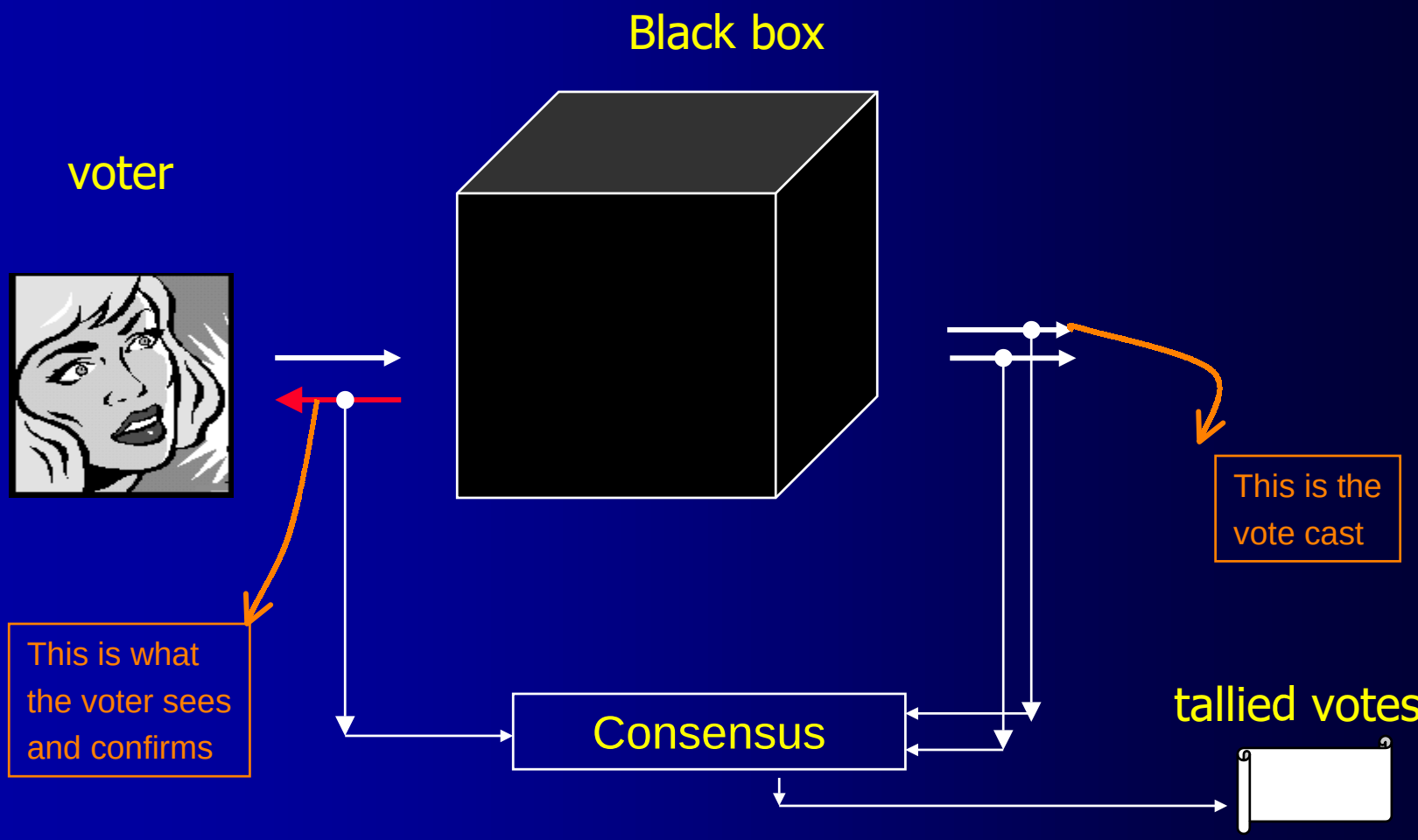
Thus,

we do not have to witness every vote, everywhere, every time.

# What We Don't Want in Voting Systems



# Working with black boxes



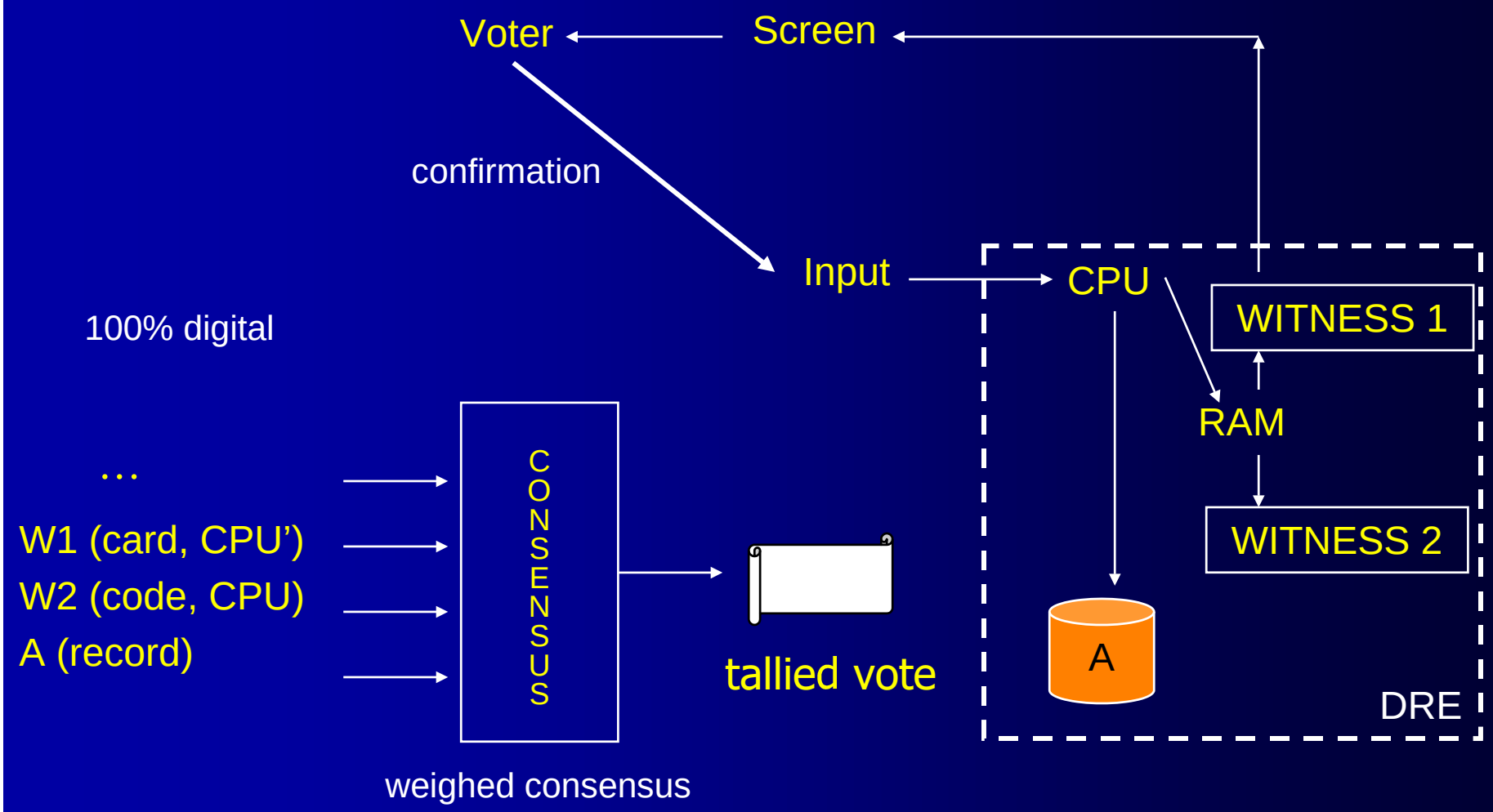
# Some comments

- One or more witnesses are used to capture the primary information: what the voter sees and confirms on the screen.
- A primary information witness can be used by itself as the voted ballot, with better reliability than the voted ballot stored in the DRE cartridge.
- However, one “strong” evidence can never be perfectly strong – it may, and will, fail.
- The objective of the witness voting system is thus NOT to rely on one “strong” evidence, which can never be perfectly strong, but to rely on several, mostly independent evidences.
- Several, mostly independent evidences can build a correction channel with enough capacity so as to correct all but an arbitrarily fraction of the errors.
- This is a new security paradigm. Instead of the “Fort Knox” approach (“make it stronger”) that relies on what becomes a single point of failure, this approach calls for a meshwork of links such that a number of links may fail at the same time without compromising accuracy and reliability.

# Voting used to to solve problems in voting

- The Witness Voting (W-V) system enhances accuracy and reliability of the underlying voting system – the W-V system behaves as a meta-voting system.
- We can have n such tiers of systems and meta-systems.
- The meta-system does not introduce any semantics (no change in meaning).
- The meta-system provides a verification of the outcome without compromising the sender's or receiver's privacy in the original tier.
- The semantics of the underlying system are maintained in the outcome, but with higher resiliency.
- Multiple confirmation screens can be used without concern.
- **Real-time auditing** – Test votes can be cast without being observable as test votes by the DRE.
- **Dynamic certification** – The meta-voting system can objectively rate the underlying voting system (as a black box) during the election in terms of accuracy and reliability, allowing for continuous grading and certification of such systems while motivating their improvement for a next election.
- **Fault Prevention** – Before reaching critical levels or compromising an election, non-performing voting systems can be shut down during the election by election officials, based on real-time, measured uncertainty.

# Low-Cost Practical Example – Card and Code Witnesses




Expected probability of compromise: W1 < W2 < A

# Summary

This paper addresses the fundamental problem in public elections (the “vote gap” problem), which is that of tallying a ballot as seen and cast by a voter.

The significant aspect is that in order to preserve election integrity, no one should be allowed to prove what ballot was cast by a voter – not even the voter. The system must be designed to allow the voter to cast any ballot within a possible selection set.

DREs (direct recording electronic voting machines) are used to exemplify a method called “witness voting” (W-V) that is 100% digital and can be used to prove, with an error margin as close to zero as desired, that the ballot seen and cast by a voter using a DRE is the ballot that will be tallied. The W-V method does not need to change the DRE, does not use paper ballots and can be applied to network voting.

The W-V method also leads to methods called “real-time auditing” and "dynamic certification,” which can be applied to “black box” voting machines, so that at the end of an election one can objectively grade each election machine and decommission those machines that do not conform with what can become well-defined performance standards of accuracy and reliability. W-V also includes fault-prevention methods.


# Voting with Witness Voting:
## Qualified Reliance on Electronic Voting

WOTE '01

Tomales Bay, California, Aug 27-30, 2001.

Presentation by:

*Ed Gerck, Ph.D.*

*egerck@safevote.com*

*CEO & VP of Technology*