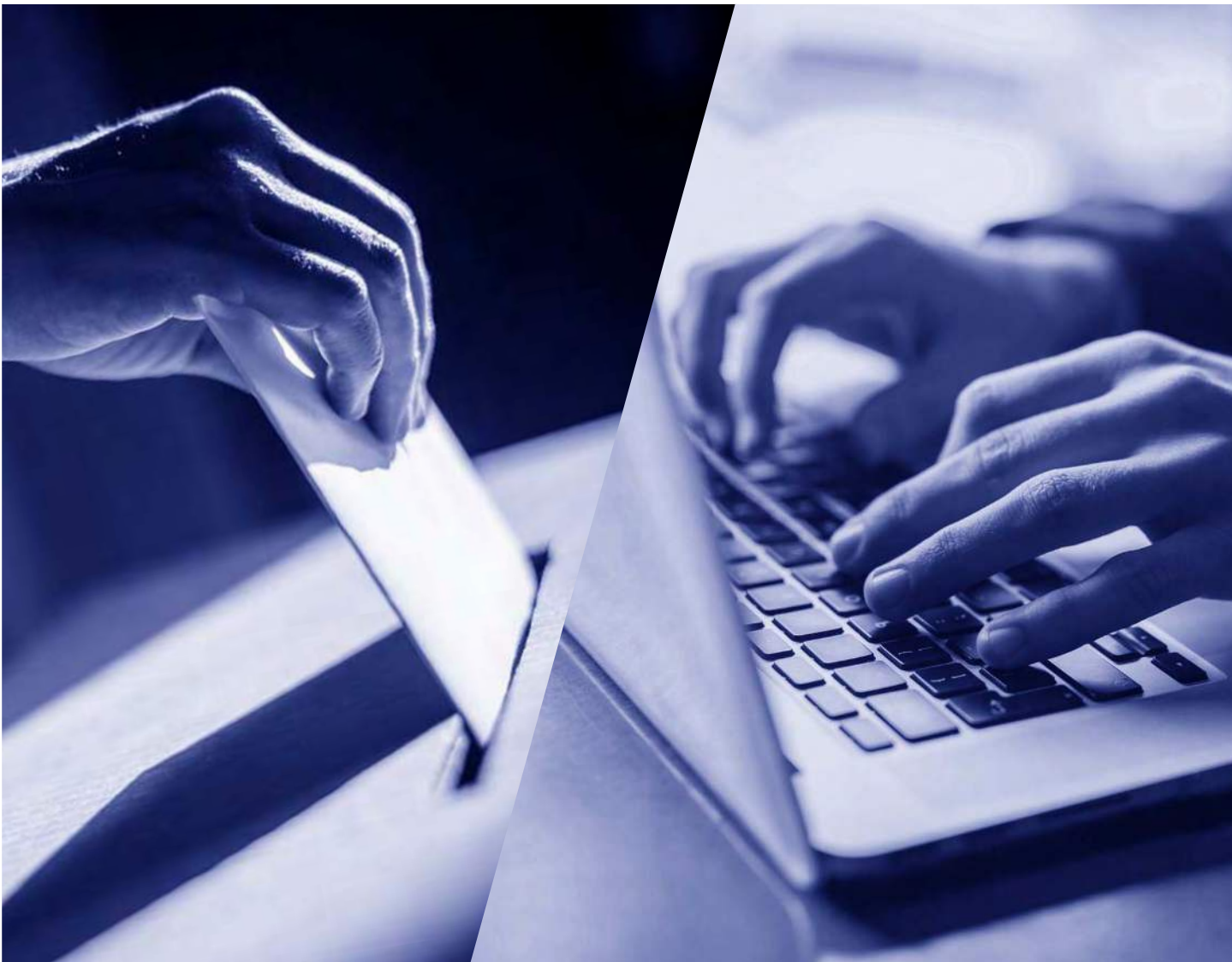# Black Box Voting vs. End-to-End Verifiable Voting

Is it possible for something to be both secret and transparent?

That paradox is one of the biggest challenges facing developers working in the world of electronic voting. On the one hand, ensuring a secure voting experience means making the process open and observable from beginning to end. On the other hand, that process can never compromise the anonymity of the votes being cast. The good news is that striking a balance between those two goals is possible.

In fact, that technology is already in use in many places around the world, with companies like Assembly Voting leading the drive to make end-to-end verifiability the new standard for secure electronic voting. Getting organizations to adopt a new, more secure style of voting just requires a new perspective on some outdated ideas and outmoded technology.

What is End-to-End Verifiability?

Voting systems with end-to-end verifiability are currently changing the way the world thinks about electronic voting. End-to-end auditable voting systems allow observers to witness and verify that they are functioning properly throughout the entire voting process. While these systems still keep elections secret and anonymous, they also provide visibility into how each vote is collected, recorded, and tabulated. For a system to qualify as fully verifiable, voters need to be able to confirm that their votes have been:

1. **Cast in the way the voter intended**
2. **Received as cast**
3. **Counted as received**

ASSEMBLY VOTING

The need for end-to-end verifiability is perhaps most obvious when considering the importance of national elections, but a verifiable, transparent process should be best practice for every democratic voting situation. A secret and verifiable means of voting is essential to:

- **Shareholder meetings**
- **Professional associations**
- **Unions and employee organizations**
- **Homeowner associations**
- **Church and school boards**

Fortunately, technological advancements in electronic voting have made end-to-end verifiability achievable in most voting scenarios. Let's take a closer look at what true verifiability looks like.

How is End-to-End Verifiability Accomplished?

Transparency needs to begin well before the first vote has even been cast. The international voting rights group NDI states that in order for any electronic voting system to be considered transparent, "the procurement, development, testing and certification of voting and counting equipment should be carried out transparently, so stakeholders are confident the machines meet relevant requirements, function properly and have the necessary security features in place." Before the vote takes place, all voting mechanisms should be accessible to any stakeholders or other concerned parties. These recommendations are just as relevant when considering online voting in both public and private arenas. In a business setting, for instance, that might include anyone from potential board members to voting employees. Any voting event should also involve trained administrators who can explain the processes, answer questions, and, as a result, dispel any doubts about integrity.

When voting is underway, transparency means allowing voters to effectively follow the journey of their votes. Transparent electronic voting systems must also employ a method that allows third-party observers to verify the accuracy of each step without revealing confidential information about individual voters. That usually means employing homomorphic encryption, a process that checks partially decrypted votes against mathematical proofs that confirm the data is correct but do not expose any personal identifiable data.

Many end-to-end verifiable systems also employ a public bulletin board. This is a place where voting and system transaction information is stored and displayed for public (re)viewing. That might include information such as:
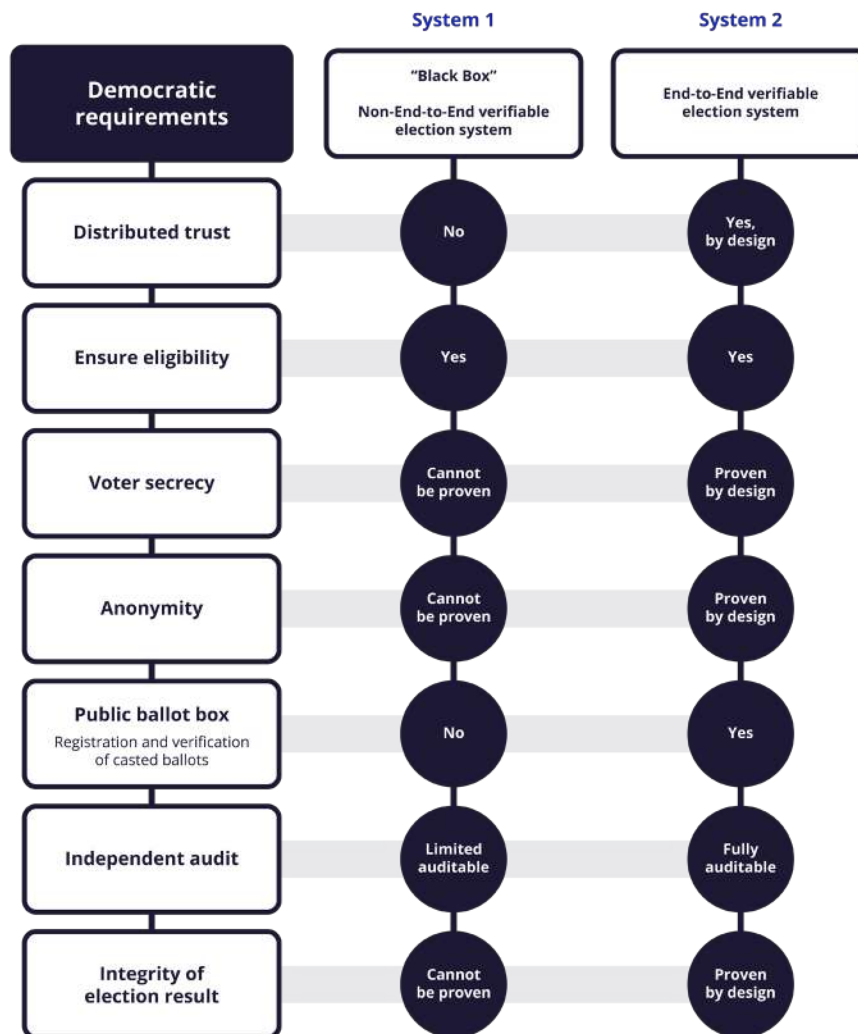
- **Details of public keys and how they are generated**
- **Auditable records of all encrypted votes**
- **Auditable results of all tallied votes**
- **Mathematical proofs that demonstrate the accuracy of all of the above**

A bulletin board serves as both a record of all voting activity, and as verifiable proof that the system is functioning properly, and all votes are being recorded correctly. The use of a hashchain can furthermore increase transparency with provable results that cannot be altered or deleted without detection.

This kind of system not only verifies that each vote has been cast, recorded, and tallied exactly as the voter intended, it also provides detection mechanisms to ensure that only valid votes are included in the count. Homomorphic encryption makes it simple for third parties such as media outlets, election observers, auditors and academics with concerns about accuracy to have a full view of the process from beginning to end.

Why Does End-to-End Verifiability Matter?

Democratic requirements	System 1 "Black Box" Non-End-to-End verifiable election system	System 2 End-to-End verifiable election system
Distributed trust	No	Yes, by design
Ensure eligibility	Yes	Yes
Voter secrecy	Cannot be proven	Proven by design
Anonymity	Cannot be proven	Proven by design
Public ballot box Registration and verification of casted ballots	No	Yes
Independent audit	Limited auditable	Fully auditable
Integrity of election result	Cannot be proven	Proven by design

Essentially, a democratic election process must comply to basic democratic requirements and End-to-End verifiable voting system is the only way to ensure this in online election services.

End-to-end verifiability is the only way to comply with the fundamental requirements of any democratic election, whether in the public or the private sector. Distributed trust, integrity by design, and verifiability are not just empty phrases. Regardless of how the election process is conducted, or whether it takes place at a physical polling station or online, these words represent important principles and actions. They constitute the difference between a legitimate, democratic election result and an untested "black-box" statement that provides no evidence of accuracy. The latter opens a potential door for election fraud, dangerous conspiracy theories, and general mistrust in the election process. A trustworthy democratic election result must be founded on evidence-based election processes to maintain legitimacy, whether the election is for directly elected political posts or for board members, employee representatives or a trade union resolution.

ASSEMBLY VOTING

What is Black Box Voting?

If you've done any research into the technology behind the world's voting systems, you've probably come across the term "black box voting." Generally speaking, this refers to systems that fit one or more of these criteria:

1.	2.	3.
Voters have little or no visibility into how their votes are recorded	**Voters have little or no visibility into how their votes are counted**	**There is no tangible record of individual votes that have been cast**

Essentially, a black box voting system is any mechanism that leaves voters or administrators uncertain whether a vote has been cast and counted as intended, and provides no means of verifying any of that information. Some sources classify all computer-based voting as black box on the assumption that electronic processes are inherently less transparent than physical voting, but that is not a useful or accurate designation in an era of increasingly sophisticated and transparent elections technology.

ASSEMBLY VOTING

Why is Black Box Voting a Problem?

Proponents of black box voting systems argue that a lack of full transparency is necessary in order to preserve the secrecy of the vote and guard against tampering. In fact, recent history offers a number of examples to the contrary. A 2018 Microsoft report on voting in the European Union, for instance, notes that both Ireland and Germany scrapped implementations of electronic voting systems in the early 2000s, largely because the technology then available in polling places did not offer enough visibility into the processes. Basically, a system that does not allow outside observers to see how it works also makes it difficult to identify if the system has been compromised or is functioning correctly.

Consider this hypothetical scenario: A company's shareholder organization votes to retain a sitting board member by a narrow margin, but some shareholders raise questions about whether their votes were received as cast. A system with end-to-end verifiability would be able to provide evidence that each of their votes was recorded correctly and cast as intended by each individual voter. A black box system may provide records of how many votes were cast when those votes were cast, and which registered voters cast votes in the election, but the accuracy of the final vote count would remain in question. That lack of transparency can lead shareholders to lose trust in the integrity of the organization. If that mistrust compels them to sell off their stock, that can have a bad impact on the company's reputation, and ultimately on its bottom line.

In recent years there have been various examples of how mistrust in the election outcomes has paved the way for democratic crises and even undemocratic responses. This is happening in both the public and the private sector, causing a huge negative impact on organization's brands and their preceived integrity as well as undermining the general trust in democratic election processes.

Moving forward in an increasingly hostile technological environment, it becomes even more important to provide end-to-end verifiability that demonstrates evidence of a fair election or voting event. As the threat landscape changes, it is essential to be able to detect attempts to tamper with the election as well as to prove the accuracy of the election outcome. Voter verification methods, distributed trust and public bulletin boards, open for public auditing, help to remove mistrust and assure the voters that their votes are counted accurately and securely.

Assembly Voting stands as a leader and evangelist for transparent, auditable, and accurate electronic voting mechanisms. It is clear that the days of black box voting that provides limited visibility are numbered. End-to-end verifiable voting is the way forward for sustainable democratic elections across the globe, and Assembly Voting will continue pushing toward a brighter, more transparent future for all democratic elections.

ASSEMBLY VOTING

About Assembly Voting

Assembly Voting was the first provider of digital elections in Denmark. Today, we have grown to become a global leading election technology provider across Europe, the USA and the rest of the world.

Assembly Voting is based on the idea of strengthening democratic participation in society and associations, through the integration of fundamental democratic processes with documented secure and user-friendly technologies.

Assembly Voting provides mathematically proven and fully documented election solutions for ministries, municipalities, professional organisations, companies, associations, etc.

Learn more about the technical solution and the election process here:
https://assemblyvoting.com/products/assembly-voting-x/

Primary systems

Assembly Voting X

The digital polling station - Proven secure online voting systems.

Assembly Conference Voting

System for "live" elections independent of physical presence.

Additional systems

Assembly Pre Election

Registration, validation and presentation of candidates.

Assembly Assist

Add-on modules that connect with Assembly Voting X to increase participation and deliver support during the election.

Facts

- First digital legislative and statutoryelections in Denmark (2001)
- More than 1000 clients across 75 countries
- 6,000+ elections
- 35 million+ voters
- 35,000+ candidate registrations
- Full service, partner and self-servicesolutions

Contact our sales department to learn more about how we can implement your next candidacy process.

ASSEMBLY VOTING