# Conversation with Gemini

**Authors:** on 12/7/2025

**-Can you judge the correctness of this statement about the Estonian i-voting system IVXV?:**

"*Could lead to a kind of massive vote buying/coercion that is never possible even in poll station e-voting; voters could be forced to copy a vote they do not even know. Imagine a scenario where an adversary controls "n" voters with a malicious VA' as in DARKDAOs (using execution attests to assure a certain code is executed, which is the malicious voting application VA' in this scenario); the adversary either perform an auction between corrupted candidates, or even worse works for another country, then sends an encrypted choice* $(g^r , y^r.v)$ *to VA' to copy. If you think you can search the anonymous ballots for suspected repetitions, VA' could add a fresh randomness to each vote* $(g^{r+r\_new},y^{r+r\_new}.v)$."

-Is the original statement accurate?

-Is the attack really feasible on large-scale?

-Do smart contracts facilitate generating and sending the encrypted vote online whether auctioned between competitors or from another adversarial country?

## Gemini

Here's my plan to tackle that topic. Let me know if you need to make changes.

(1) Research the fundamental challenges and vulnerabilities associated with vote buying and coercion in various e-voting system architectures, including remote and in-person models.
(2) Investigate the concept of malicious voting applications (VA') and explore how decentralized autonomous organizations (DAOs) or similar structures could be exploited to facilitate large-scale vote manipulation, such as in 'DARKDAOs'.
(3) Analyze the role of execution attestation in securing e-voting systems and how an adversary might subvert or misuse it to ensure the execution of a malicious voting application (VA') without detection.
(4) Examine cryptographic protocols and system designs aimed at preventing or detecting vote buying and coercion in anonymous and encrypted e-voting schemes.
(5) Evaluate the impact of adding fresh randomness to encrypted votes on the ability to detect coerced or repeated votes, and its implications for the overall auditability and integrity of the election.
(6) Compare the susceptibility of different e-voting models (e.g., internet voting, blockchain-based voting, kiosk voting) to the specific type of attack scenario described, focusing on the client-side vulnerabilities.
(7) Identify proposed technical and procedural countermeasures, including cryptographic techniques and secure software development practices, designed to mitigate the risks of malicious client-side applications and subverted attestation in e-voting.
(8) Synthesize the findings to provide a comprehensive analysis of the feasibility and potential impact of the described vote buying/coercion scenario, along with a summary of effective prevention and detection strategies.

**Answer:**

You've outlined a highly sophisticated and concerning attack scenario, which indeed combines several advanced techniques to subvert e-voting integrity. Let's break down each part of your question.

## 1 Is the original statement accurate?

## 2 Is the attack really feasible on large-scale?

## 3 Do smart contracts facilitate generating and sending the encrypted vote online whether auctioned between competitors or from another adversarial country?

Yes, smart contracts can indeed facilitate various aspects of such a sophisticated attack, including the generation and transmission of encrypted votes, and potentially the coordination of illicit payments.

- **Smart Contracts for Voting:** Smart contracts are fundamental to blockchain-based voting systems, managing processes like voter authentication, vote recording, and tallying. They can define governance rules and automate decisions.
- **Generating and Sending Encrypted Votes:** Blockchain-based voting systems often integrate cryptographic techniques like homomorphic encryption with smart contracts to ensure vote privacy and integrity. Votes are typically encrypted before being cast and recorded on the blockchain. Smart contracts can handle these encrypted transactions.
- **Auctioning Votes/Illicit Payments:** Smart contracts can be programmed to implement auction logic. While the research doesn't explicitly detail "auctions between corrupted candidates" for votes in a general election, smart contracts can enforce financial incentives for voter participation, such as requiring deposits that are refunded upon casting a vote. This mechanism could theoretically be adapted for illicit vote-buying schemes, where the smart contract facilitates the payment upon "verification" of a coerced vote (e.g., through a subverted attestation mechanism). Smart contracts are designed to execute automatically once conditions are met, making them suitable for coordinating such illicit transactions without human intermediaries.
- **Coordination by Adversarial Countries:** State-sponsored actors have demonstrated capabilities in leveraging blockchain technology for illicit financial activities, including stealing virtual currency using fraudulently obtained identities. While direct evidence of smart contracts being used by adversarial countries for large-scale vote manipulation in e-voting is not explicitly detailed, the ability of smart contracts to automate complex, transparent, and immutable transactions, combined with state-level interest in cyber warfare and election interference, makes them a plausible tool for coordinating and executing such schemes. The transparent and immutable nature of blockchain, while beneficial for legitimate uses, could also be leveraged by adversaries to ensure "proof" of illicit transactions if not properly secured.

**In conclusion**, your scenario outlines a highly sophisticated and technically informed attack that leverages known vulnerabilities and properties of e-voting systems, client-side security, TEEs, and blockchain technology. The feasibility of such an attack on a large scale is a significant concern, underscoring the complex challenges in securing modern elections.

Sources and related content


What to Do If You Connect to a Malicious dApp: Step-by-step Guide | Tangem Blog

tangem.com

Auction Smart Contracts: A Deep Dive | by Lea Lobanov | Coinmonks | Medium

medium.com

How does malware spread? Top 5 ways malware gets into your network - Emsisoft

www.emsisoft.com

Going from bad to worse: from Internet voting to blockchain voting | Journal of Cybersecurity

academic.oup.com

Secure Voting Website Using Ethereum and Smart Contracts - MDPI

www.mdpi.com