Remote voting system and blockchain in voting

January 26, 2021

In news : Election Commission to begin the mock trials for remote voting, it is also exploring the possibility of using blockchain technology for the purpose of enabling remote elections.

Background

Election Commission had, last month, held an online conference in collaboration with the Tamil Nadu e-Governance Agency ("TNeGA") and IIT Madras, through which they explored the possibility of using blockchain technology for the purpose of enabling remote elections

Key highlights

- During the National Voters Day, the Election Commission announced that it will begin mock trials for remote voting.
- The ECI has been working with IIT Madras to create the technology backbone for remote voting.
- The advent of EVMs has laid the platform for it. To begin with, remote voting may be possible only at designated centres outside a voter's constituency.

Blockchain technology and remote voting

A blockchain is a distributed ledger of information which is replicated across various nodes on a "peer-to-peer" network for the purpose of ensuring integrity and verifiability of data stored on the ledger. Blockchain ledgers have traditionally been used as supporting structures for cryptocurrencies, such as Bitcoin and Ethereum; however, their use in non-cryptocurrency applications too has seen a steady

rise, with some solutions allowing individuals and companies to draft legally-binding “smart contracts,” enabling detailed monitoring of supply chain networks, and several projects focused on enabling remote voting and elections.

Arguments in favour of remote voting

- Once the system proves robust and technology advances, it may eventually be possible to vote from home.
- It would especially help senior citizens and physically challenged voters.
- It would enable migrants to vote and also lessen parochialism in election voting patterns, thereby helping the cause of national integration.
- The envisioned solution might also be useful for some remotely-stationed members of the Indian armed forces, though it should be noted that, for the most part, vote casting has not been an issue for those serving in even the remotest of places including the Siachen Glacier, which, given its altitude, is considered to be the ‘highest battleground’ on the planet.

Key issues and concerns with the blockchain-based remote voting systems

- **With this system,** electors would still have to physically reach a designated venue in order to cast their vote, adding that systems would use “white-listed IP devices on dedicated internet lines”, and that the system would make use of the biometric attributes of electors.

- Digitisation and interconnectivity introduce additional points of failure external to the processes which exist in the present day.
- The system envisioned by the Election Commission is perhaps only slightly more acceptable than a fully remote, app-based voting system

- The systems used in such low-stakes elections have suffered several blunders too, some of which could have been catastrophic if they had gone undetected.
- Blockchain solutions rely heavily on the proper implementation of cryptographic protocols.
- If any shortcomings exist in an implementation, it might stand to potentially unmask the identity and voting preferences of electors, or worse yet, allow an individual to cast a vote as someone else.
    - For example, in Russia, during the vote on the recent controversial constitutional amendment ushered in by Russian President Vladimir Putin, citizens were able to cast their vote online.
    - While the voting process was still under way, a Russian media outlet reported that it was possible to access and decrypt the votes stored on the blockchain due to a flaw in cryptographic implementation, which could have been used to unmask the votes cast by electors.
- The requirement of physical presence and biometric authentication may not necessarily make a remote voting system invulnerable to attacks either.
- An attacker may be able to clone the biometric attributes required for authenticating as another individual and cast a vote on their behalf.
- Physical implants or software backdoors placed on an individual system could allow attackers to collect and deduce voting choices of individuals.
- The provisioning of a dedicated line may make the infrastructure less prone to outages, it may also make it increasingly prone to targeted Denial-of-Service attacks (where an attacker would be in a position to block traffic from the system, effectively preventing, or at the very least delaying the registration of votes).
- More attack scenarios that the system might be vulnerable to will slowly become evident when additional

details about the hypothesised system are disclosed.

- Apart from lingering security issues, digitised systems may also stand to exclude and disenfranchise certain individuals due to flaws in interdependent platforms, flaws in system design, as well as general failures caused by external factors.
- Naturally, the more levers that are involved in the operation of a system, the more prone it would become to possible malfunction.

Way forward

If the only problem that is to be solved is the one of ballot portability, then perhaps technological solutions which involve setting up entirely new, untested voting infrastructure may not be the answer. Political engagement could perhaps be improved by introducing and improving upon other methods, such as postal ballots or proxy voting. Another proposed solution to this issue includes the creation of a ‘One Nation, One Voter ID’ system, though it is unclear whether such a radical (and costly) exercise would be required at all for the mere purpose of allowing individuals to vote out of their home State.