BLOCKSUITS

BLOCKCHAIN SYSTEMS, DIGITAL IDENTITIES AND ELECTION FRAMEWORKS

Authored by:
Mustafa Rajkotwala
Samaksh Khanna

Background

India has been exploring the possibilities of implementing a remote voting system through technologies such as blockchain since the past few years. The Election Commission of India ('**ECI**') has taken up this idea with enthusiasm, and has been working towards initiatives that could bring a blockchain based remote voting system to reality. Recently, the ECI conducted a discussion with various government, state and private industry stakeholders in order to explore the idea of a nation-wide remote election system. The primary agenda of the discussion revolved around the current setbacks that are faced in physical voting systems around the country in terms of inability to reach physical polling stations and inaccuracy in counting of voting data. In such a case, a remote voting on a blockchain medium could promote transparency, security and accountability in terms of each vote that is casted.

Remote voting through the blockchain system would include similar practices that are followed in cryptocurrency transactions, with the only difference being that instead of a virtual currency, there is a virtual token representing a 'vote'. This would entail a peer-to-peer technology that would utilise encryption and a write-once model (a model in which information, once written, cannot be modified. This assures that the data cannot be tampered with once it is written). The electronic ledger will allow private and secured registration information and ballots to be transmitted over the internet. However, the ballot rolls and the counting of the votes would be displayed on public domain, in order to ensure transparency and prevent fraudulent practices. Countries such as the United States, Argentina, Sierra Leone, Russia, Estonia and Thailand in the past have utilised the blockchain methods for conducting voting processes for their citizens, with a fair share of positives and negatives deriving consequentially.

Functioning of remote voting system

The functioning of a remote voting system is explained through the following scenario:

Person A is a registered voter in New Delhi (a union territory in India) and has a place of residence and place of work in the state of Maharashtra (a state in India). Through the e-voting system, the resident of Maharashtra would be able to cast his vote on Election Day by not travelling to the State of Delhi specifically. For the said scenario, a hypothetical process is explained as under:

Step 1 – Identity Verification

In this step, the nation of Estonia serves an excellent example. The Government of Estonia is one of the first countries to implement a truly online e-voting platform. They use 'smart digital identity cards' and 'personal card readers' for person wise authentication of identity. In the Indian scenario, we propose a similar but simpler model considering the infrastructural status of Indian states and union territories. For the purpose of identity verification, the government may create an application which shall interact with the authentication server, which creates identities for voters on the blockchain and also authenticates the token provided to it while voting, say **BlockSuits Votes**. BlockSuits Votes would contain information of all voters in a database. The voter would then enter her/his personally identifiable information (**'PII'**) for the purpose of verification and BlockSuits Votes shall also capture an image of the voter for ensuring the identity of the candidate. Such PII may contain documentation and biometric data along with contact information. Upon verification of such information and scanning of the voter's picture, BlockSuits Votes would create an account by generating a login ID and giving the voter the discretion to choose the password. The login ID and password shall not be linked to the voter's PII and have a separate database. Since the user ID would not be linked to the voter data base, it shall ensure anonymity and privacy. If any step is missing or the data entered by the voter for the purpose of verification, such as biometric information, is incorrect then the account for the voter shall not be created.

Step 2- Voting Process

The above explained process requires the voter to register on BlockSuits Votes, an application designed to facilitate identity verification. The data on BlockSuits Votes would be utilised by the blockchain system deployed to verify the identity of the voter on the day of the voting. A moving image may be captured of the voter to match it with the initial data on BlockSuits Votes during registration of account. The reason for providing a moving image of the voter is to identify any 'duress', 'fear' or 'coercion' through the deployment of Artificial Intelligence ('AI') and Machine Learning (**'ML'**) systems. If there is a detection of the above, then the voting mechanism stops, providing a division of time before another voting session can be logged in. On the same happening after the 3rd (third) try, the voter is locked out of the voting process.

Application of blockchain to e-vote casting

The actual system of voting on the day of the voting would be based on a blockchain. Once the logging in process is complete, the system would create a public key which would be sent to the authentication server. This public key shall be used to create an account for the user on the blockchain system to follow the voting process and to initiate the vote. Like Ethereum blockchain, where ether is added to initiate a transaction, on the blockchain voting system a specific amount of an alternative to ethers, say BlockSuits Coin can be added which shall be the currency which enables the voter to vote on the blockchain. While using blockchain, an important concept of an arbitration server comes into play. An arbitration server is an intermediary that sends the users' vote to a blockchain node. After issuing of the BlockSuits Coin, the BlockSuits Votes (authentication server) would send a token back to the voter which the voter shall send to the arbitration server and verify the same with the authentication server. After this process, the arbitration server shall provide the public key of the blockchain node, to which the vote would be sent, to the voter. The voter would cast his encrypted vote using the public key, and send it to the arbitration server. The vote here would not be disclosed as vote would be encrypted and the arbitration server would not be able to read the vote. After this, the arbitration server would send the encrypted vote to the appropriate node. The node would then decrypt the message using the private key and send a specific amount of BlockSuits Coin from the voter's account to the candidate's blockchain account. In this case, the amount of BlockSuits Coin could also be sent to the abstain account if the voter wants to abstain the vote. All such transactions would then be verified using a smart contract for duplicity and validity, post which the transaction may be sent to other nodes in the blockchain network.

Application of blockchain to e-vote counting

In a case that the laws of a country allow for an interim result, the voter may use her/his public key to verify whether their vote was counted. One of the nodes of the blockchain could be made publicly available and such a node would not have the ability to add any transactions which can be implemented through smart contracts. The counting of votes shall be done through analysis of BlockSuits Coins. Since voters are provided with a specific value of BlockSuits Coins which are being transacted to the candidates account, the candidate with the maximum BlockSuits Coins, keeping in mind the BlockSuits Coins sent to the abstain account, in their account shall win the election.

How far along is India in implementing a trial phase?

The Telangana government has shown immense interest towards implementing an experimental run towards an e-voting idea, and raised a point towards building the voter's trust towards such remote voting systems by aiming at a holistic user inclusion. In May 2019, they had published a 'Blockchain Policy Report' (**'BPR'**), where they discussed the relevancy of blockchain in a wide variety of domains, including tax filings, voting, land registry setups, utilisation of healthcare facilities, creation of tamper-proof voting records, registration of vehicle and licenses, fraud-proof welfare-scheme disbursements, and digital identities for individuals, such as refugees, who lack government-issued identity documents. BPR also advocated for the use of biometric facial recognition for voter identity authentication, as well as connecting the voter's phone number and IMEI to voter ID for verification in rural voting systems.

In February 2020, the ECI had collaborated with Indian Institute of Technology, Madras (**'IIT-M'**) to develop a new technology which will allow electors to vote from far away cities without going to the designated polling station of their respective constituencies via a blockchain system. The model followed by them was that of a 'two-way' blockchain remote voting process that would entail voter identification and authorisation on the Electoral Registration Officer Network (ERO Net) using biometric data and web cameras for facial recognition, followed by a blockchain based e-ballot generation, which would convert into a vote once the hash code would be generated on its execution (as explained in the above process). The encrypted remote votes casted would once again be validated at the pre-counting stage to ensure that they have neither been decrypted, nor tampered with or replaced. In course of this, the Election Commissioner, Mr. Sunil Arora has proposed to link voter IDs with the Aadhaar Card if India adopts a blockchain voting model as a solution for the longer run.

International perspective

In the United States, third-party applications such as *Votem* and *Voatz* have assisted in conducting such polling processes, alongside local county governments of West Virginia, Denver and Utah. *Votem* worked on a model where the voters check that their individual votes were counted, whereas *Voatz* supplemented the blockchain framework with biometric identity verification, using smartphones' and tablets' built-in fingerprint readers and facial recognition to authenticate voters. In Argentina, a local party start-up called *Democracy. Earth* had conducted a blockchain voting system prototype on the basis of an open-sourced model. In 2019, Sierra Leone, alongside a blockchain company called *Agora* conducted nation-wide elections on an immutable ledger system, with its information open to public access. Russia, had its governmental authorities conducted runs of blockchain-based elections in 2019 and 2020, respectively.

As we look at the lessons that can be inferred from these systems, let us first delve onto positive side of the spectrum. Blockchain voting has shown to reduce geographical barriers and increase turnout in voting numbers, promote security towards recording of votes as opposed to physical tampering, an enhanced efficiency in counting voting numbers and minimising errors and easing the overall process for the voter by utilising basic features such as facial recognition and biometric identification protocols. For example, the county voting in the USA counties helped increase the remote voters' turnout from 3% to 5%. Sierra Leone saw 70% of its citizens voting at the elections. As a whole, to counter the difficulties and citizen's growing anxiety towards traditional offline ballot elections, the shift towards an online system on the blockchain has shown promise.

On the other hand, the negatives which this framework presents easily convinces us to take a step back and look at the actual effectiveness of this idea, and ponder upon whether there are additional complications that arise out of the same. Primary issues that arise are cyber-security vulnerabilities, and malware attacks by third parties. Furthermore, although the blockchain framework promises transparency, operations which are carried forward by third-party vendors (although at a governmental authority's behest) can give rise to tampering and ineffective results. For example, the Voatz application, in reports, has been touted to compromise a voter's data under an attack, wherein the latterwould able to observe, suppress, and alter votes nearly at will. Network attacks could also reveal where a given user was voting and potentially suppress votes in the process. In such a case, if the blockchain displays all the votes to be on public domain, a simple hack into the system puts thousands of people's data at risk.

A 2018 report titled "Email and Internet Voting: The Overlooked Threat to Election Security" by the US National Election Defense Council (**'NEDC'**) along with various organisations looked at the various threats posed by the adoption of a blockchain system. Their findings included the point of how tampering a paper-ballot system would act as a one-time damage, but a blockchain system being infected by attacks would affect the voters' computers with malware or the computers in the elections office that handle and count ballots, would lead to long-term damages and large-scale corruption.

Way Forward for India

The fundamental purpose of a blockchain system is to decentralise and anonymise the process of transactions. This is done with the help of public-generated addresses and private 'keys'. If such information of an individual comes into the eyes of the public or a hacker, the entire security element of the blockchain is breached. As governments then prefer to centralise the digital identities of their individuals for voting processes, their data becomes vulnerable to the authorities and the third-party body that is facilitating such a transaction. A solution in opposition to such a system is an end-to-end verifiable voting system which has newly gained attention of cryptographers around the globe. However, we are yet to see if any government/authority puts this system into practice in the future.

As we grapple with understanding the effectiveness and scope of implementing blockchain elections in a country like India, we need to address more fundamental issues alongside the ones that have already been mentioned above. We have a dearth of computer and internet-access around nation, alongside the illiteracy and ignorance of citizens towards the adoption of such advanced technologies. Although the blockchain election system comes with promise to develop and ease hassles, looking at the issues faced in precedents around the globe, coupled with problems unique to us, the future of a complete reliance on this system does seems to be a distant future.