Evoting Using Blockchain Technology

Amrita Jyoti, Rashmi Mishra, Rupa Rani, and Ravi Kalra

Abstract Voting is the fundamental right of each and every citizen in a democracy. Perhaps, it is the very basis of a democracy. Democracy means a government for the people, of the people, and by the people. This means many rights such as freedom of speech, right to information, to name a few. But the right that defines a democracy is voting. It means that those who are willing to form a government and serve the people stand as candidates, and the people are allowed to choose, who they wish to be served from (i.e., the government). Looking at how imperative voting is, it is also essential that all citizens are able to cast their votes during the election. Now here comes the problem, especially in countries like India. Some people are not available in the city at the time of voting, they may be traveling, etc.; for the others, the voting center might be very far away from their houses. And in India, with the vast multitude of population, a large fraction of people is not even able to receive their voter ID cards (Barański et al. in Appl Sci 10:7606, 2020 [1]). Also, some people may be handicapped and hence are not able to vote. There is a one clear solution to all this, "Evoting," a concept that will be elaborated in this paper, stating how it is done, what technology it uses, and its advantages over the currently used voting methods.

Keywords Voting · Blockchain · Evoting · Ballots · Electronic voting machine · Public distributed ledger · Mining · Miners · Transaction · Immutable · Proof of work · Cryptocurrency · Encryption · Democracy · Election · Ganache · Truffle · JavaScript · MetaMask · NPM · Solidity

A. Jyoti (✉)
Ajay Kumar Garg Engineering College, Ghaziabad, U.P, India

R. Mishra · R. Rani · R. Kalra
Krishna Engineering College, Mohan Nagar, Ghaziabad, U.P, India
e-mail: rupa.rani@lloydcollege.in

R. Kalra
e-mail: ravi.kalra@lloydcollege.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

X.-Z. Gao et al. (eds.), *Advances in Computational Intelligence and Communication Technology*, Lecture Notes in Networks and Systems 399,
https://doi.org/10.1007/978-981-16-9756-2_7

1 Introduction

The problems stated in the abstract are prevalent all over the world, with the system that is used for voting. Currently, voting is carried out in 2 ways:

1.1 Paper Ballots

Here, the voter needs to select/mark the party he/she wants to vote for on a piece of paper and then put the paper in a box. This results in lots of paper usage, thereby making this method very less eco-friendly due to the carbon footprint it has. Also, since the votes are cast on paper, the process of counting takes place manually [2]. This has some problems associated with it.

Manual Errors: The process of counting such a large number of votes is tedious, and the people can get lethargic while counting the votes which can result in the officials' losing track of the counting. So, the counting loses its reliability and credibility, which is so very important in voting.

Cost Of Voting: Manual counting means the counting will be done by humans. And this human labor will be needed to be paid some wage. This may sound a little easy in countries like India and China (where the cost of labor is very less), but in countries like the USA the cost of labor is extremely high; this does not seem feasible. With the labor comes a cost, and this cost becomes a disadvantage in ballot-based Evoting.

1.2 Less Eco-Friendly

Also, since this method of voting uses paper, it has lots of carbon footprint associated with it, directly proportional to the paper produced in making the ballots, and then resource consumption in printing the ballot on the paper.

1.3 Time Taken to Announce Results

Now, since the counting is manual (which it is in most cases), the time taken to announce the results is also very high. And, even if we consider the time taken to count the votes using machines, it would still be considerably high.

2 EVM Machines

EVM is an initialism for electronic voting machine. In this case, the voter needs to go to the voting center and press the button of the party of the voter's interest, and the vote is cast electronically [3]. In this case also, the following problems arise:

2.1 VVPAT

VVPAT is an initialism for Voter-Verified Paper Audit Trail. This is a system in which the cast vote of the voter is printed on a piece of paper, which is displayed through a transparent screen to the voter. This allows the voter to verify whether his/her vote has been correctly recorded. Now, this VVPAT system (which is mostly employed with the EVM, except for some rare cases) brings with it certain issues. First, it brings back the carbon footprint that was also an associated problem with paper ballot voting system. Second, it necessitates the integration of a printing device with the display system of the EVM, thereby increasing the consumption of electricity and other resources [4].

2.2 Increased Cost

The EVMs are operated electronically and also require other devices such as printers integrated with them. This leads to costs such as electricity, printer inks, paper procurement for the VVPAT paper slips, and also a very big cost which is called the maintenance cost of the machines. Also, keeping the machines secure is a cost (the storage cost).

2.3 Danger of Tampering

In the recent elections, there have been claims by some political parties that the EVMs can be tampered and hacked. If the EVM is hacked by any means, there would be no credibility and reliability of the voting conducted; hence, the essence of a democracy is lost.

2.4 *Time for Result*

One more problem with EVM voting is the tedious process of vote counting. Though electronic, this method also takes some time in vote counting as all the EVMs from the different locations would be collected at one central place, and then the results of the different EVMs would be added up. Now, one major issue arises at this point. If, at the time of vote counting, there is a dispute, then the EVM total would have to be matched with the VVPAT paper total, and for this, the VVPAT paper ballots would have to be counted, thereby resulting in the EVM voting degrading to the cumbersome paper ballot voting task.

3 What is Blockchain

A blockchain is a collection of blocks, each of which stores some information. A block in a blockchain takes its reference from the previous block in the chain to verify and perform changes to the data in the previous block that are reflected in the current block. Each such change in a blockchain, wherein a new block is added to the chain, is called a transaction. Now, this chain of blocks is distributed to everyone in the world and hence is known as a public distributed ledger (Fig. 1).

Now, there are some agents who add new blocks to a blockchain, called "miners." These miners have to solve a complex mathematical problem to add a block to the chain [6]. This is called "proof of work." After the miner has solved the problem, the block gets added to the chain (this is called "mining"), and the miner gets a reward

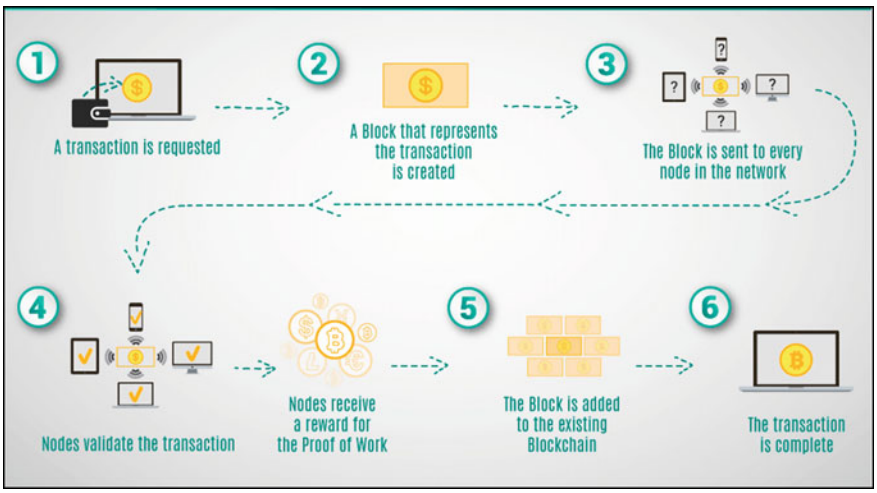

Fig. 1 How blockchain works [5]

in the form of cryptocurrency. All cryptocurrencies (e.g., Bitcoin, Ethereum, etc.) work on the concept of blockchain.

4 How is Blockchain Used in Evoting

Let us see how the above-discussed blockchain technology is used in Evoting. This concept is implemented in a different type of web called the distributed web (d-web). The difference between normal web and d-web is that the web is centralized in nature, whereas the d-web is distributed in nature. In the case of the web (which is currently being used by everyone), we follow the client–server paradigm. In this case, the user is the client and the entity where the actual data stored is called the server. When the client requires any information, a request is sent to an entity in the network that contains that information (i.e., server). The information may be anything such as a web page, a pdf, a document, and an image. Now, if the server has the information, it sends that information to the client [7]. But in this case, there is always the risk of central failure, as all the information resides in the server, and failure of the server would mean failure of the entire system. Enter the d-web. In d-web, there is no central entity governing everything. But anything and everything a user may require is distributed among all the nodes in the network. This acts more like a peer-to-peer network. So now, if a node requires some information, then its request can be served by all the other nodes in the network. These other nodes have either full copies of the document or parts of it (in this case, the client's request can be fulfilled by multiple nodes having the copies). This enables the big, combined computing power of the different nodes to be utilized in the most optimum way [8]. It also eliminates the need of depending on a central authority for running the show. Also, we will not have to give ownership of any document to any entity (as in case of a cloud). And the publication process becomes much easier. There is no need to own a server in the d-web. Taking all the above facts into consideration, the process of Evoting would be carried out in this distributed web. The voter may access the online polling booth in two ways, either through an application that accesses the d-web (i.e., a d-app or a distributed application) or through their web browsers using an interface to access the d-web (e.g., MetaMask, etc.). Now, at the side of the organizer, there is the task of maintaining the database of the eligible voters, the creation of an election, and the maintenance of the vote blockchain (a blockchain that is a record of the votes cast).

Before the election, the election organizer will create an election. On the election day, the voter will go to the voting app (in case of d-app usage) or would log in to the voting portal (in case of web browser usage). For verifying the identity, the voter would need to enter credentials such as mobile number and Aadhaar number. Then, an one-time password (OTP) would be sent to the voter's mobile. Upon validating the OTP, the voter will be directed to the Voter Registration Page. Here, upon requesting for registration, the voter credentials would be sent to the organizer, who will verify whether the voter is eligible to vote from the voters' database. If the voter is found to be eligible, the voter's details are added to voters' blockchain (a blockchain storing the

registered voters' details and also the votes cast by them) and a smart contract will be issued to the voter in the form of an electronic ballot. The voter would then cast his/her vote on this electronic ballot and submit the vote. On pressing the submit button, another OTP would be sent to the voter's mobile number to confirm submission of the vote. The voter will enter this OTP and log out of the voting page. This vote would also be added to the voters' blockchain. Since the voters' blockchain is a public distributed ledger, the voter can audit the votes any time, while also maintaining the privacy of other voters. Hence, fair results are ensured. Also, the results can be immediately declared after the voting with no manual counting process required, thereby completely eliminating the chances of errors due to counting. This process has no carbon footprint as no paper ballots are used in the voting process. Also, there is no cost of running the heavy machinery and no consumption of expensive resources and the costs associated with them. And most importantly, this method eliminates the need of physically going to a polling booth for voting. All that is needed is a stable Internet connection, and the job is done, sitting at home, hassle-free [9].

5 Phases of Evoting Using Blockchain (Explained with the Help of Flowcharts)

The entire process of Evoting using the blockchain technology can be divided into the following two phases.

5.1 Registration Phase

In this phase, the following events occur: The election organizer will create an election on the election app. The voter will download an Evoting app or would use the voting portal over the distributed web through web browser. He/she will log in using credentials like mobile number and Aadhaar card number on the app for registration. An one-time password (OTP) would be received on the voter's mobile number. Upon entering the correct OTP, the voter will be directed to the registration page. The voter would request for registration. Now, the election authority would validate whether the voter exists in the voters' database. If yes, the voter's details would be added to the voters' blockchain and a smart contract will be issued to the voter in the form of a ballot, on which the voter can cast his/her vote on the election day, using their app (see Fig. 2).

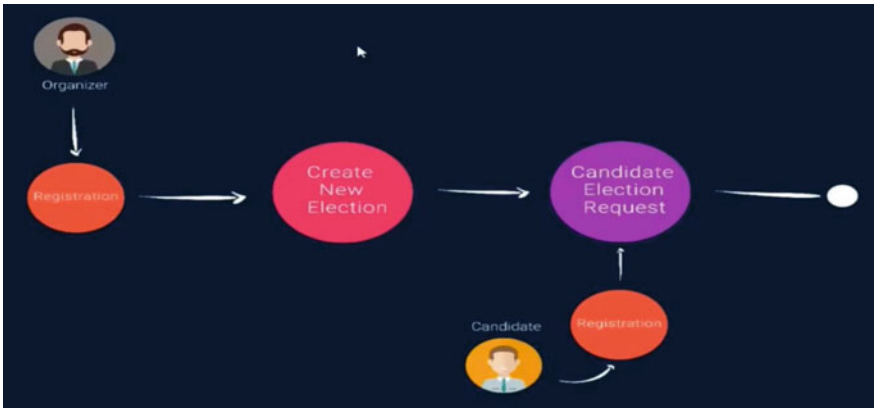

Fig. 2 Registration phase in evoting [10]

6 Voting Phase

First, this phase takes place on the day of the election. Secondly, the voter opens his/her app and requests to vote. Then, the election authority checks whether the user is valid and if this is their first vote. If the above details are verified, the voter is allowed to vote. The voter then casts his/her vote. Then, an one-time password (OTP) is sent to the voter's phone for confirming the vote submission. On successfully entering the OTP, the vote gets added to the voters' blockchain (see Fig. 3).

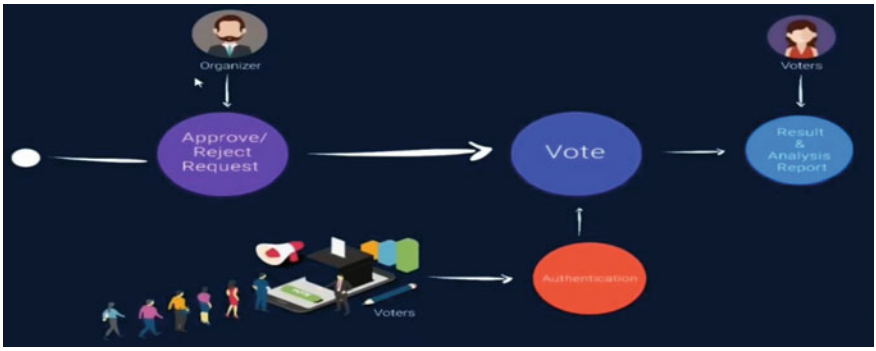

Fig. 3 Voting phase in evoting [10]

7 Tools and Technologies Used

This system of Evoting can be implemented with the following tools and technologies (as explained in this section in the form of a classification of hardware and software requirements):

7.1 Hardware Requirements

For implementation of the proposed voting method, the organizer of the election would need a personal computer (Windows 7 onward). It needs to be a 64-bit machine. As far as the voter side is concerned, the voter can vote in two ways. Using a personal computer (laptop, desktop, etc., Windows 7 onward for Microsoft users and all versions of operating systems for Mac users; the machine needs to be 64 bits) either in case of voting using the web portal [11] or in case the voter wishes to use the d-app, he/she may use a smartphone (Android or iOS both would work).

7.2 Software Requirements

This section only concerns with the software requirements of the election organizers. Since this voting method would be implemented on the distributed web, the organizer would require some advanced tools and technologies to create and host the elections, and accept votes in the blockchain, keeping them secure and maintaining the reliability and credibility of the elections.

The following are the tools required to conduct election using the blockchain technology.

NPM: NPM is an initialism for Node Package Manager. NPM can be used in two ways, as an online platform and as a command line tool. As an online platform, NPM allows one to publish and share tools made using the JavaScript language [12]. These tools can be used in browsers (i.e., in front end), servers (i.e., at the back end), or even the command line. As a command line tool, NPM enables users to interact with the aforementioned online platforms. So, one can do the following things with NPM as a command line tool:

It enables one to **install and uninstall packages**. A package is a tool someone created and uploaded to the NPM online platform. One can think of a package as a building block of an application or an even bigger package.

NPM can also be used for **version management**. Every package has a version. As the package grows and improves, the version of the package also changes. With NPM, one can easily keep the packages in one's project up to date. It even lets one switch to another package version, whenever one wants.

It is used for **dependency management**. Many packages that people create are built on top of other packages. Dependencies are packages on top of which other packages are built. Instead of the developer searching for each and every dependency and installing them one by one, he/she can use a single command to install a package with all its dependencies. This means that NPM does all the hard work for the developer.

Truffle framework: Truffle framework is a very powerful tool that is used to work with Ethereum smart contracts. It is used for deploying, compilation, and linking of smart contracts, manages networks and packages, and also, provides a testing platform for automated contracts, etc.

Ganache: Ganache was previously known as testrpc. It can be used in two ways, as a command line and as a user interface. It uses a virtual blockchain, and then, it establishes ten standard Ethereum addresses with all the blocks in the chain along with private keys. Ganache then preloads them with hundred ether each (theses are simulated ether). There is no mining required in Ganache. Instead, the task is made much easier with Ganache automatically confirming every transaction. It is convenient to use with a vast variety of operating systems like Windows, Linux, and Mac.

MetaMask: MetaMask is an open-source tool. It is extremely user-friendly tool. It has a graphical user interface (GUI) and performs all transactions in the Ethereum cryptocurrency. The common web browsers (like Google Chrome, Mozilla Firefox, and the like) are not capable of running or one can say, accessing the distributed web (d-web) on their own.

They need a support for that, and MetaMask is that support. MetaMask allows Ethereal DApps to run on one's normal system browser without the user node having the need to become a complete Ethereum node. One can say that MetaMask is a bridge between the normal system browser and the distributed web.

Solidity: Solidity is a language that uses JavaScript style syntax for contracts. It is used to generate EVM (here, EVM stands for the Ethereum Voting Machine) machine level code and then further convert it into simple instructions. It works with four value types. These are address, integer, string, and Boolean. Solidity uses the same operators as those used in JavaScript. It is a high-level language.

8 Advantages of Evoting Using Blockchain Over Other Systems

The advantages of Evoting using blockchain are:

8.1 Auditability

The voter can audit all the ballots in the chain, while maintaining the other voters' privacy. This becomes possible because the voters' blockchain is a public distributed ledger, granting access to all the voters in the voters' list.

8.2 Transparency

Maximum people, in the current voting system, think that their vote is not considered due to some fraudulent practices that may be taking place at the time of vote count. But this problem is tackled properly by the method proposed in this paper. The voters' blockchain is transparent, and the voter comes to know whether or not his/her vote is counted. All this becomes possible due to the distributed nature of the blockchain.

8.3 Immutability

Now, in everything that involves the web, there is always a risk of changing the data contained in the data repository. Switch to blockchain. The blockchain is immutable.

8.4 No Risk of Hackin

In the proposed system, wherein everything is shared in public, there is always a risk of hacking and altering of the data. The voters' blockchain cannot be altered by hackers owing to the encryption applied to every block in the chain. Also, if at all the data of one block is changed, the hacker will need to change all the previous blocks in the chain.

8.5 Secure and Hassle-Free

The main problem with offline voting systems was that the voter had to physically go to the polling booth for casting his/her vote. But now, one can sit in the comforts of one's home or anywhere in the world and vote for one's desired candidate. Also, no security concerns owing to the blockchain technology. Just a stable Internet connection leads to an extremely secure and hassle-free method of voting.

8.6 No Cost of Resources

There is no need for the organizer to procure expensive machines or paper and pay for the heavy amount of electricity and other resources consumed for voting. All the organizer needs are a voting d-app, a setup to host the voters' database and the voters' blockchain, and an OTP generation equipment. And all the voter needs are a mobile app and an Internet connection to vote.

8.7 No Need to Go to Polling Booths

The most concerning issue with offline voting systems was that the voter had to physically go to the polling booth for casting his/her vote. But now, one can sit in the comforts of one's home or anywhere in the world and vote for one's desired candidate. The voter can vote from any part of the world.

8.8 Reliability

Since every vote is stored in the voters' blockchain, every time a voter casts his/her vote, the d-app checks the voters' blockchain for a vote cast by the voter. If no vote from the particular voter is found, it means that the voter is voting for the first time. Only then is the voter allowed to vote. Otherwise, he/she is rejected. Hence, every voter can vote only once.

8.9 No Fraudulent Practices

Since the blocks in the blockchain are encrypted, hence no one can tamper them. Also, the blocks are distributed in public. So, there cannot be any manipulation in the counting of the votes. In short, there is no fraud in voting.

8.10 Immediate Result Declaration

The voting results are announced immediately after voting is completed. There is no requirement of manual counting (as in the case of paper ballot voting) or even machine counting (as in the case of EVMs). So, it is very time saving.

8.11 Environment-Friendly

In this system of voting, no paper is used (which are used in both, paper ballot voting and EVMs). Also, there is no electricity consumption, which is very high in the case of voting using EVMs. Therefore, this method is more environment-friendly, as carbon footprint is negligible. Since there is no need to go physically to the polling booth, there is no use of vehicles, no traffic jams at the polling centers, and hence no fuel consumption (something that contributed largely to environmental pollution).

8.12 No Labor Cost for Voting

Since no manual counting of votes takes place, and also, no vote totaling is done (as in the case of EVMs where the votes of the individual machines are totaled), there is no dispute in the vote count (as happens sometimes with EVMs), and there is no need of any human labor to count the votes [13].

9 Conclusion

Hence, we have a hassle-free system of voting, more secure than anything the world could ever imagine. Extremely, user-friendly voting environment, no problems of going to any polling booths physically, more transparent than ever, no frauds, voting from the comforts of your home, or even while traveling to some other city or abroad, what else does a voter want. There cannot be an easier way for a voter to exercise his/her rights. This practically feasible voting system comes as a boon to all handicapped people who face extreme difficulties in voting and prefer not to vote. Also, in this time of the COVID-19 pandemic, where it is very unsafe to step out of one's house, this system of electronic voting comes to a voter's rescue. Apart from this, Evoting also provides immediate election results. This paper provides a deep insight to the basic concepts required to understand Evoting using the blockchain technology, and also, how it can actually be carried out on a large scale [14]. Apart from a government election, it can also be used to carry out elections in offices, colleges, and any places requiring choosing representatives through an election.

References

1. Barański S, Szymański J, Sobecki A, Gil D, Mora H (2020) Practical I-voting on stellar blockchain. Appl Sci 10:7606. https://doi.org/10.3390/app10217606

2. Lalam N, Nithinn MS, Jebakumar R (2020). BEVS—blockchain based E-voting system. Int J Adv Sci Technol 29(9s):6241–6249. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/20208
3. Wang B, Sun J, He Y, Pang D, Lu N (2018) Large-scale election based on blockchain. Proc Comput Sci 129:234–237
4. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where is current research on blockchain technology?—a systematic review. PLOS ONE 11(10)
5. https://datascience.foundation/img/pdf_images/fig_2_blockchain_architecture_diagram.png
6. Barnes A, Brake C, Perry T (2018) Digital voting with the use of blockchain technology. Available https://www.economist.com/sites/default/files/plymouth.pdf [Nov 20, 2018]
7. Hjálmarsson FÞ, Hreiðarsson GK, Hamdaqa M, Hjálmtýsson G (2018) Blockchain-based E-voting system In: 2018 IEEE 11th international conference on cloud computing (CLOUD), San Francisco, CA, pp 983–986
8. Kshetri N, Voas J (2018);Blockchain enabled E- voting. www.computer.org/software
9. Çabuk UC, Adıgüzel E, Karaarslan E (2018); A survey on feasibility and suitability of blockchain techniques for the E-voting systems. Int J Adv Res Comput Commun Eng
10. https://youtu.be/WLwfCgLHK5Y
11. Cruz JP (a), Kaji Y(b) (2017) E-voting system based on the bitcoin protocol and blind signatures. IPSJ Trans Mathem Model Appl 10(1):14–22
12. Madise Ü, Martens T (2006) E-voting in Estonia 2005. In: The first practice of countrywide binding Internet voting in the world. Electronic Voting, vol 86
13. Green T, Sarrasin O, Baur R et al (2016) From stigmatized immigrants to radical right voting: a multilevel study on the role of threat and contact. Polit Psychol 37(4):1–22
14. Burton C, Culnane C, Schneider S (2016) vVote: verifiable electronic voting in practice. IEEE Secur Priv 14(4):64–73