Long Read: How blockchain can make electronic voting more secure




While a great deal of our lives have moved online, voting by and large still takes place using paper ballots. **Amrita Dhillon**, **Grammateia Kotsialou**, **Peter McBurney** *and* **Luke Riley** *write that controversies over the expected surge of mail-in ballots in the US November elections due to the COVID-19 pandemic underscore the need to modernise the mechanics of voting. They argue that blockchain technology can enhance efforts to move to electronic voting by offering greater security and transparency, which may increase needed trust in election systems.*

As the US presidential election approaches, one of the largest impact of the COVID-19 crisis has been on how people vote. Many voters have become wary of going to polling places for fear that they will be exposed to the virus at election sites filled with other voters. The only other options are online voting, generally conducted by email in a limited number of places, and postal ballots, now a subject of political controversy in the US. In the run-up to the November elections, questions are growing over whether a surge of ballots will overwhelm the postal service, and whether cutbacks to the service and efforts to discredit mail-in voting by President Donald Trump are politically motivated to undermine both election turnout and confidence in the results.

For the first 50 years of US elections, voting took place in public, by voice. Eligible voters went to the local courthouse to vote. Since the move to the anonymous paper ballots of today, voting technology has changed little, making the way that we select our leaders look antiquated compared to the growing use of the Internet and other forms of contemporary digital communication. Yet, where adopted, electronic voting has shown clear benefits. For example, research in Brazil has shown that the adoption of electronic voting reduced residual votes, and led to greater de facto enfranchisement of mainly uneducated voters– leading, as a result, to increased government spending on healthcare services. Recent research in India showed that the use of electronic voting machines has reduced electoral fraud.

Fears blocking progress

Fears of large-scale manipulation of online votes has kept back progress in making change. Indeed, very few countries use online voting at all, and most of them that do, use some version of Electronic Voting Machines (EVMs) which require voters to go to a polling booth and show identification before inputting their vote on the EVM. There are obvious advantages to EVMs. The speed of counting, especially in large countries like India and Brazil, has made EVMs a necessity and an important cost-saving measure. By contrast, many mature democracies have not embraced online voting, due to fears of hacking and fraud. Some countries have actively discontinued their use (e.g. the Netherlands in 2005). Indeed, Estonia is one of the few countries that has successfully run its elections electronically but with a full paper ballot backup. Estonian citizens can also cast their vote physically in the polling booth, and, if they do, the paper ballot supersedes any electronic vote they may have cast.

But EVMs and centralised online voting systems like that of Estonia do not actually solve one of the major issues facing democracies: ensuring trust in the election authority. While this is arguably a problem facing new democracies, it seems to be an important concern now in mature democracies, as the situation in the US illustrates. Moreover, EVMs do not reduce the burden of voting. Voters still need to go to the booth – an issue during the ongoing pandemic. Therefore, EVMs have less impact on turnout than an e-voting system could have.

A possible technological solution

Our recent research addresses the issues that affect electronic voting. We examined the ways in which a centralised online voting system would be vulnerable to fraud, and argue that a blockchain-based system offers a solution.

Date originally posted: 2020-09-25

Permalink: https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

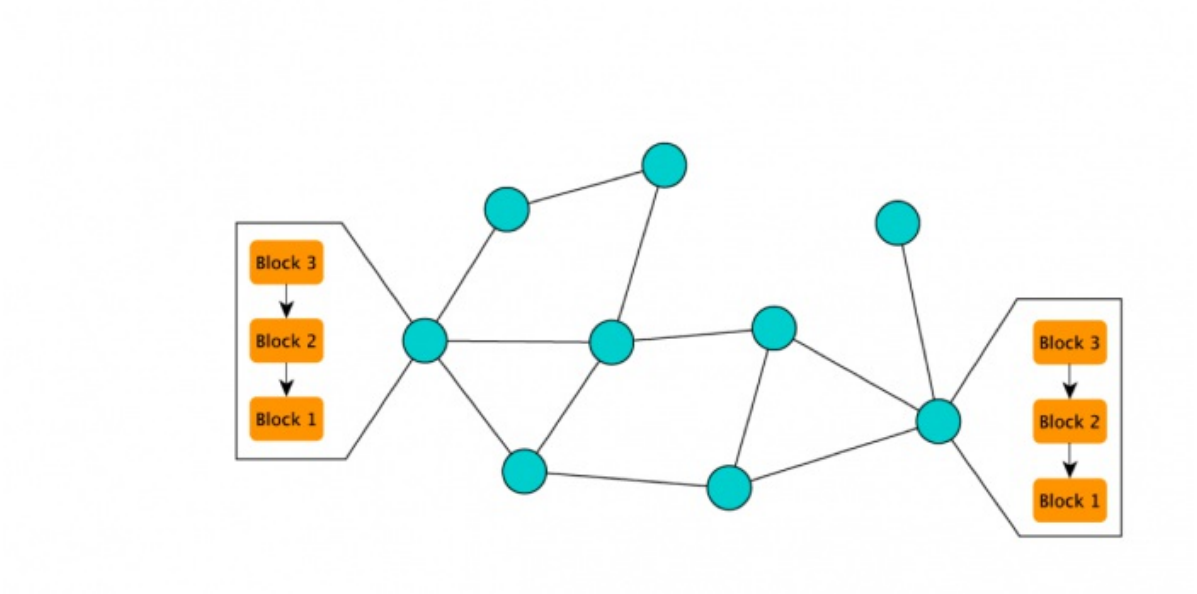
Blog homepage: https://blogs.lse.ac.uk/usappblog/

A blockchain is a type of distributed ledger technology (DLT) – a shared ledger (file/database) of records or transactions that is open to inspection by every participant, and is not subject to any form of central control. Bitcoin is the most famous example of a blockchain application. A blockchain is distinguished by the rules it follows if ledgers do not tally, or if inconsistencies arise. The technology stores information sequentially in "blocks" in an ordered chain, with "validators" (those who have appropriate rights in the shared ledger) verifying and storing each transaction. Nothing in the verified record of the transaction can be altered, and the system offers a fully auditable history of all transactions.

In April 2019, some members of our team launched a trial project of a blockchain powered electronic voting system. Funded by the Engineering and Physical Sciences Research Council, the trial aims to enhance the vote verifiability features of an online voting platform. The project uses the voting system owned by Electoral Reform Services (since taken over by Civica Election Services) together with the project's open source Verify My Vote platform to provide verifiability. The blockchain technology underpinning this platform allows voters to verify that their votes are counted, and that the votes are recorded correctly without compromising their own anonymity. Moreover, anyone can check that the counting was done correctly without compromising the secrecy of the ballots. While a single authority (Civica) oversees the current centralised system of voting in its elections, it is now possible to distribute control of the election among several trustees, which might increase voters' faith in the results.

Figure 1 shows a version of a blockchain. The blue circles represent the validators (nodes) in a network, and orange rectangles represent the three blocks, indicating that every validator (node) in the network has the same agreed-upon information.

Figure 1



Source: Dhillon et al 2020

The premise of blockchain technology is that decentralising the validation of information among multiple authorities (the blue circles in Figure 1) makes it much more difficult to manipulate elections. In essence, the fact that every vote needs to pass the scrutiny of several validators in the network increases the cost (and decreases the likelihood) of electoral fraud. Indeed, a large number of election stakeholders would need to work together for fraud to occur.

Date originally posted: 2020-09-25

Permalink: https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

Blog homepage: https://blogs.lse.ac.uk/usappblog/

Photo* by *Phillip Goldsberry* on *Unsplash

In a *permissioned* system the validators would be known to voters. For example, party representatives from different parties, who likely have low incentives to collude, would ensure trust in the system. In addition, a blockchain-based system can allow independent vote-monitoring bodies to audit the vote counting and codes used to make sure that the system is free from fraud – something that current centralised systems do not offer. Blockchains can be incorporated into the voting architecture right from the stage of electoral registration to vote storage and vote counting. At each stage they prevent a single agent from making changes without agreement among a specified subset of the entire network of permissioned validators (nodes). The downside of these additional security checks is the cost of running additional servers.

That said, the blockchain cannot solve all the possible types of election fraud. A network of authorised validators cannot check whether votes come from genuine users, but it can check other key concerns: that the vote is technically valid, that no double counting occurs, and that the vote comes from an authorised place. In Estonia, for example, voters can cast their votes from anywhere in the world using an identity card with a computer-readable microchip; yet there is still no guarantee that the entry point (i.e. the computer the voter uses) is free from malware.

Addressing the potential for vote buying

Voting outside a secure booth creates space for voter intimidation or vote buying. Vote-buying transactions rely on being able to prove that the vote went to the right candidate. While this is difficult (though not impossible) with current systems, vote buying might well become easier with online voting. Social scientists have a role to play here, first, in designing incentive systems that discourage vote buying or intimidation. In Estonia, for example, any individual can change his vote multiple times before the close of the election, making it more difficult and costly for a vote buyer to check that the vote seller has indeed voted for the candidate he promised to support. Second, most types of election fraud have been found to occur in election booths (e.g. in India), in the counting of votes (e.g. in the Honduras general election 2017). Further research is needed to assess how and where the main types of election fraud occurs.

While there is a lot of ongoing research on building scalable blockchain-based voting systems, as yet, none of these systems have been used in a national election. Versions are being used in smaller elections for limited purposes. For example, in 2016 the Blockchain Technologies Corporation worked with Republican Presidential candidate Rand Paul to record the Iowa caucus results onto the blockchain for long-term storage, via its VoteWatcher product. In the US, a number of states allow electronic voting, some with blockchain-based apps.

Boosting integrity

Date originally posted: 2020-09-25

Permalink: https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

Blog homepage: https://blogs.lse.ac.uk/usappblog/

The benefits of a successful secure and transparent online voting system are clear. Such a system would do away with the issues of postal ballots being delayed, waylaid, or lost en route. It would reduce the time needed to count votes, and allow for a much higher level of accessibility to the system, and therefore higher de facto enfranchisement. Finally, new and better voting rules can be implemented. For example, in referendums, voters can securely delegate votes to more informed friends. It is also possible to develop voting rules that allow multiple votes and incentivize more informed voters to use those votes. The blockchain allows a secure design of such new voting rules.

The blockchain can do nothing to prevent misinformation or fake news from affecting voters in important elections. But, it could go a long way in ensuring that the issues that the world faces right now in terms of boosting the integrity of the election authorities and voting processes.

With the development of a scalable blockchain-based system, there need be no concerns about postal votes being deliberately delayed, or about non-verifiability of votes in existing electronic voting systems. At least some of the challenges facing e-voting – maintaining records securely, and ensuring auditability and transparency – can be solved. Better systems are certainly possible. So, what is holding back greater investment into more research for the design of secure online voting systems? Integrity of elections is the single most important activity for democratic governments.

- *This article is based on the paper, 'Voting over Distributed Ledger: An interdisciplinary perspective'.*

Please read our comments policy before commenting.

Note: This article gives the views of the author, and not the position of USAPP– American Politics and Policy, nor of the London School of Economics.

Shortened URL for this post: **https://bit.ly/3cvMuyY**

About the authors

Amrita Dhillon – *King's College London*
Amrita Dhillon is a Professor of Economics in the Department of Political Economy. Her main field of research is political economy.

Grammateia Kotsialou – *now LSE Fellow in Mathematics (Operations Research)*
Grammateia Kotsialou was a Research Associate in the Department of Political Economy at King's College London during this study.

Peter McBurney – *King's College London*
Peter McBurney is Professor of Computer Science and former Head of the Department of Informatics in the Faculty of Natural and Mathematical Sciences of King's College London. His primary areas of research are in AI and Computational Finance.

Luke Riley – *Quant Network*
Luke Riley is Head of Innovation in Quant Network. Luke Riley was a Research Associate in the Department of Informatics at King's College London during this study.

Date originally posted: 2020-09-25

Permalink: https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

Blog homepage: https://blogs.lse.ac.uk/usappblog/

Date originally posted: 2020-09-25

Permalink: https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

Blog homepage: https://blogs.lse.ac.uk/usappblog/