THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

July 27, 2021

Blockchain vs Public Bulletin Board for Integrity of Elections and Electoral Rolls

By: Prashant Agrawal,Subodh Sharma,Subhashis Banerjee

When the Election Commission is the sole decider of a public ledger, the use of Blockchain to conduct polls & maintain voter lists may result in an unverifiable & highly insecure solution. A simpler cryptographic-secured public bulletin board will suffice.

There have been several recent reports in the media indicating that the Election Commission of India (ECI) is contemplating using Blockchain technology for conducting elections in India in near future (Biswas, 2021; Rakheja, 2021; Mitra, 2021; PTI, 2021a,b, 2020; Mishra, 2020; Hunt, 2020; Bhardwaj, 2020).

A Blockchain is a distributed public ledger maintained by multiple peers over a peer-to-peer network, each of whom can have a full copy of the ledger. Transactions in the ledger are added in chunks—or *blocks*—such that the blocks are chained together to form a linear history of transactions. On the assumption that the network is controlled by an honest majority of peers, the ledger history cannot be modified by any minority of dishonest peers. This guarantee is achieved by a variety of cryptographic techniques that achieve consensus among the peers on what should be considered as the “official” history. The record of transactions can be made public for increased transparency, or for enhanced privacy they can be encrypted from public viewing.

It appears that Blockchain is being considered for three possible scenarios:

1. App-based internet voting, where votes may be treated similar to cryptocurrencies and the votes cast may be stored encrypted as transactions on a Blockchain in a transparent and immutable manner. Tallies may then be computed securely on the Blockchain, possibly directly in an encrypted domain.
2. Precinct voting in secure polling booths, but storing the cast votes and tallying on a Blockchain.
3. Maintaining electoral rolls on Blockchains, especially in the context of remote (out-of-station) voting.

In this note we review the suitability of each of these scenarios. While internet voting—with or without Blockchain—is widely considered unsuitable for large elections (Rivest, 2001; Tufekci, 2019; National Academies of Sciences, Engineering and Medicine, 2018), the claims that Blockchains will make elections and electoral rolls more secure often originate from flawed understanding of both Blockchain properties and electoral requirements. In particular, we argue that while transparency, immutability and data encryption may be necessary for elections and electoral rolls, they are by no means sufficient. Besides, these desiderata can be met by the much simpler and well known cryptographic construct of a public bulletin board (Heather and Lundin, 2009)—which we also describe below—and using Blockchains may actually be insecure and unsafe (Park et al., 2021).

1. Internet voting

App-based internet voting is considered unsafe for three main reasons.

First, it is practically almost impossible to make large-scale internet voting—with votes cast from people’s homes and other private places—coercion free. Given the gender and other social realities, the possibility of vote coercion even from family members cannot be ruled out. There is also the possibility of other coercers insisting on “screen sharing” during voting using any of the readily available software tools, which is virtually impossible to prevent in practice.

> [P]ublic verifiability and auditability—the two most crucial concerns in public elections—are always in doubt when votes are only recorded electronically.

Second, it is impossible to assume that a general voter will have access to a device or an app that can be trusted to carry out the necessary voting tasks—for example, encrypting the vote and casting it over the internet—securely and privately. This is commonly known as the “secure platform problem” (Rivest, 2001). A voter may own electronic devices like smartphones, tablets, laptops and other computers, but is seldom aware of their internal functioning or is in full control of the underlying hardware, operating system or the application. In most situations there is no way for a voter to ensure that a genuine untampered version is running. As such, it is impossible to guarantee that these devices will not compromise vote secrecy or even carry out the necessary functions for casting a vote correctly. As has often been pointed out, “cryptography is not the problem. The problem is interfacing the voter to the cryptography” (Rivest, 2001).

Third, public verifiability and auditability—the two most crucial concerns in public elections—are always in doubt when votes are only recorded electronically. While ruling against electronic voting the German Constitutional Court made the following observation (NDI, 2009):

> The use of voting machines which electronically record the voters’ votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject . The legislature is not prevented from using electronic voting machines in elections if the possibility of a reliable examination of correctness, which is constitutionally prescribed, is safeguarded. A complementary examination by the voter, by the electoral bodies or the general public is possible for example with electronic voting machines in which the votes are recorded in another way beside electronic storage.

The principle of ‘evidence-based elections’ makes it imperative that “election officials should not only find the true winner(s) of an election, but... also provide the electorate convincing evidence that they did.” (Park et al., 2021).

A necessary condition for elections to be auditable is that they should be *software independent*, which demands that “an undetected change or error in a system’s software cannot cause an undetectable change in the election outcome” (Rivest, 2008). This is not to say that software should not be used, but that it should be possible to detect any intended or unintended malfunctions by a well-defined audit protocol. This, in turn, makes it imperative to either use a voter-verified paper audit trail (VVPAT) or issue cryptographically secure secrecy preserving receipts to voters for their cast vote (Bernhard et al., 2017). The observations of the German Constitutional Court clearly makes the latter difficult, and the former is possible only for precinct voting. In view of this, in a recent report the national academies in the United States recommended against internet voting and suggested conducting elections—electronically or otherwise—where votes should (also) be recorded using human readable paper ballots (National Academies of Sciences, Engineering and Medicine, 2018).

2. Recording votes on a Blockchain vs on a public bulletin board

The term Blockchain is often used, “confusingly, to refer to a wide range of technologies, including distributed databases, hashing, digital signatures, and sometimes even multiparty computation and zero-knowledge proofs” (Park et al., 2021). A Blockchain implements the cryptographic concept of an *append-only public bulletin board* (Heather and Lundin, 2009) where data can be put up by multiple writers—sometimes encrypted—for public viewing and verification by all. It has two main properties:

1. What may be added on to the bulletin board is decided using a distributed *consensus* protocol by multiple mutually adversarial (or, at least non-colluding) participating trustees (peers). Anybody can be a trustee in a *permission-less* Blockchain, whereas a *permissioned* Blockchain can only have a pre-identified set of trustees,
2. The append-only bulletin board is unalterable, even by the maintainers. This is achieved by distributing the bulletin board such that each participant trustee has access to the entire bulletin board and by using cryptographic protections that guarantee that the bulletin board is immutable.

Note that the above two properties by themselves do not ensure that elections become safe; actually they are somewhat orthogonal to correctness of voting. Proclaiming elections to be correct would require providing publicly verifiable guarantees— even against possible insider attacks—that votes are *cast as intended*, *recorded as cast* and *counted as recorded*.

A permissioned Blockchain may be highly insecure when there are no multiple mutually adversarial entities to ensure the integrity of the bulletin board by consensus, and the ECI is the sole authority to decide on what information should be displayed on the bulletin boards. That would tantamount to reposing unverifiable trust in the ECI. In fact, the possibility of collusion among the trustees always remains in permissioned Blockchains, and `51% attacks’—where dishonest peers form the majority in the Blockchain network—have also been orchestrated on permission-less ones (Proskauer - Blockchain and the Law, 2020).

Actually, which votes should be tallied must depend on non-repudiable records of cast votes— either receipts issued to voters after they have successfully cast their votes, or voter-verified paper records (e.g., VVPATs) or both—making any consensus protocol among multiple peers for deciding on recording and tallying of votes to be unnecessary (Park et al., 2021). The ECI's obligation to account for every issued or printed record should automatically determine which votes should be tallied.

However, putting up this information transparently on a cryptographically secure public bulletin board is a welcome idea, and indeed it is common in many election protocols (Bernhard et al., 2017). Implementing a full Blockchain when all that is required is a public bulletin board not only unnecessarily adds to the complexity but it may actually make the process unsafe.

3. An append-only public bulletin board

An append-only, immutable (tamper-proof) public (web) bulletin board (Heather and Lundin, 2009), in which data can only be added at the end but never deleted, is a publicly readable sequence of bulletins that can be defined in terms of the following properties:

Certified publishing: A public (web) bulletin board has certified publishing if whenever readers retrieve the contents of the board, they can determine with certainty (obtain a formal proof) for each bulletin on the board,

1. the identity of the (sub) authority that published the bulletin.
2. the time of the publication within a pre-specified tolerance bound.

Failure to determine either of the above with certainty will indicate malfeasance or corruption of the bulletin board.

Unalterable history: A web bulletin board has unalterable history if, whenever a reader retrieves the contents of the board at two different time instances, she is able to verify that the board read at the later instance has exactly the same content as previously at the first instance (i.e., it is unaltered), except for possibly having some additional new bulletins appended at the end (that is, the board at the first instance is a prefix of the board at the second instance). Also, all readers see a consistent common history. If this is not the case, it indicates malfeasance or that the board has become corrupted.

(In the Appendix we briefly describe for the interested reader how such immutable and transparent bulletin boards may be realised.)

3.1 Privacy of records

There is always an inherent tension between privacy and public transparency. The public web bulletin boards may be made privacy preserving by replacing the clear text messages on the bulletin boards either with their encryptions, or with their hashes (cryptographic digests that make the original messages unalterable, see the Appendix below) computed using a suitable publicly committed hash function.

In case the messages are encrypted, properties about them can be proved using *zero-knowledge proofs* (Goldwasser et al., 1985) like in cryptocurrencies. A zero-knowledge proof shows credibly (provides a mathematical proof) that some statement is true without leaking any other auxiliary information in the process. For example, a zero-knowledge proof can convince a verifier that a ciphertext encrypts a valid vote without revealing any information about the vote itself.

4. Electoral rolls on public bulletin boards

In a recent report of the Citizens' Commission on Elections, Mander and Ramani (2021) have pointed out several problems of exclusion and disenfranchisement that plague electoral rolls in India. Whereas processes for inclusion—proactively identifying all eligible voters and making sure that they are able to vote, irrespective of whether they apply or not—require being particularly mindful of marginalised communities and careful process design at local community levels, some of the other problems related to exclusion and duplicate entries can be addressed by transparent and effective data processing.

We make some suggestions for organisation and processing of electoral roll data that do not require Blockchains but only public bulletin boards to ensure that

1. All applications for inclusion in electoral rolls—whether by voters themselves, or by their representatives on their behalf—are correctly processed,
2. There are no spurious deletions from the electoral rolls,

3. There are no duplicate or false entries in the electoral rolls.

We propose to ensure the integrity of the electoral rolls by maintaining records in a manner that enables complete transparency and public verifiability of all decisions regarding enrolment, updates and deletions.

We suggest that the Election Commission of India (ECI) should maintain two public bulletin boards for each constituency—at a block/ward level granularity—which should be updated as and when changes occur.

1. **Bulletin board of electoral rolls:** This should be a self-contained bulletin board of the entire electoral roll—updated with all additions, deletions and changes till date—where each entry is timestamped and digitally signed by a competent authority in the ECI. Deletions and changes to existing entries should be made by appending fresh entries containing back-references to the original entry. The last entry in the bulletin board should override all relevant previous entries. This bulletin board should be used to create the official master electoral roll correct up to the time of the last update, and it should be possible to publicly determine the list of valid voters on any date from the bulletin board.
2. **Bulletin board of transaction records:** This should contain

1. the sequence of all enrolment applications received and enrolment records generated by the Electoral Registration Officers (ERO), and the processing information including reasons for acceptance or rejection
2. the sequence of all change or deletion requests generated, and the processing information clearly citing the reasons for the change or deletion

For every application of enrolment, update or deletion, the concerned authority in the ECI should be obligated to issue a digitally signed receipt using which a voter (or her representative) should be able to search for her application processing status on the bulletin boards. Missing processing information for a signed receipt will indicate a failure of the ECI to fulfil an obligation. Every entry in the append-only bulletin boards should be timestamped and digitally signed by a concerned competent authority. Any member of the public should be able to verify the authenticity and the integrity of the bulletin boards. Authorised entities (may even be everybody) should be able to carry out search, deduplication and audit operations on the bulletin boards.

> [T]here is no theory to substantiate that publishing only image records of electoral rolls—as is the current practice of the ECI—protects privacy..

The bulletin boards may be made privacy preserving by replacing the messages with their hashes in the bulletins. Hashes not only hide the underlying message but also ensure that the original message cannot be altered. Access to the original messages may only be given to a restricted set of authorised entities who may be empowered to audit after authentication. It is to be noted that there is no theory to substantiate that publishing only image records of electoral rolls—as is the current practice of the ECI—protects privacy, and it only serves to make searching the database difficult for an honest operator.

Similar public bulletin boards may also be considered for maintaining applications and processing records of out-of-station voters if and when a remote voting scheme for migrant voters is implemented.

5. Conclusions

We have explained the notions of a Blockchain and an append-only public bulletin board, and have argued that for the common functions in elections and maintenance of electoral rolls the former may be an overkill and a simpler implementation of the latter will suffice. We have also argued that when there is only one authority (ECI) to oversee an election, using a Blockchain may, in fact, be insecure.

Email addresses of authors: {prashant,svs,suban}@cse.iitd.ac.in, suban@ashoka.edu.in

References:

Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach. Public evidence from secret ballots. In *Electronic*

Voting - Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings, pages 84–109, 2017. doi: 10.1007/978-3-319-68687-5\ 6. https://doi.org/10.1007/ 978-3-319-68687-5 6.

Deeksha Bhardwaj. Election commission's tech advisory panel to assess options for remote voting. https://www.hindustantimes.com/india-news/election-commission-s-tech-advisorypanel-to-assess-options-for-remote-voting/story-DmIfzwM1QTCHyM7lu8vf3J.html, 2020. [Online September 12, 2020].

Atanu Biswas. From EVMs to Blockchain-based e-voting? https://www.newindianexpress.com/ opinions/2021/apr/26/from-evms-to-blockchain-based-e-voting-2294834.html, 2021. [Online April 26, 2021].

S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 291–304, New York, NY, USA, 1985. ACM. ISBN 0-89791-151-2. doi: 10.1145/22145.22178. http://doi.acm.org/10.1145/22145.22178.

James Heather and David Lundin. The append-only web bulletin board. In Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, editors, *Formal Aspects in Security and Trust*, pages 242–256, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. ISBN 978-3-642-01465-9. https://dl.acm.org/doi/10.1007/978-3-642-01465-9_16

Mia Hunt. India to develop blockchain voting system. https://www.globalgovernmentforum.com/indiato-develop-blockchain-voting-system/ , 2020. [Online February 17, 2020].

Harsh Mander and Venkatesan Ramani. "Electoral Roll and Exclusion of Vulnerable Sections from Voting". In Justice (Retd.) Madan Lokur, Wajahat Habibullah, Justice (Retd.) Hariparanthaman, Arun Kumar, Subhashis Banerjee, Pamela Philipose, Sundar Burra, and M. G. Devasahayam, editors, *An Inquiry into India's Election System: Report of the Citizens' Commission on Elections (Volume II: Are Elections in India Free and Fair?)*. 2021. https://tinyurl.com/m2hhv2w

Shaily Mishra. Experts debate using blockchain for remote voting in India. https://www. sundayguardianlive.com/news/experts-debate-using-blockchain-remote-voting-india, 2020. [Online October 3, 2020].

Siuli Mitra. Election Commission of India working with IIT Madras and CDAC for a more efficient voting system. https://static.psa.gov.in/psa-prod/psacustom files/Election%20Commission% 20of%20India-IIT%20Madras.pdf, 2021. [Online April 21, 2021; Accessed June 4, 2021].

National Academies of Sciences, Engineering and Medicine. *Securing the Vote: Protecting American Democracy*. The National Academies Press, Washington, DC, 2018. ISBN 978-0-309-47647-8. doi: 10.17226/25120. https://www.nap.edu/catalog/25120/securing-the-vote-protectingamerican-democracy.

NDI. The Constitutionality of Electronic Voting in Germany. https://www.ndi.org/e-voting-guide/ examples/constitutionality-of-electronic-voting-germany, 2009. [Accessed June 8, 2020].

Sunoo Park, Michael Specter, Neha Narula, and Ronald L Rivest. Going from bad to worse: from Internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1), 02 2021. ISSN 2057-2085. doi: 10.1093/cybsec/tyaa025. https://academic.oup.com/cybersecurity/article-pdf/7/1/ tyaa025/36276521/tyaa025.pdf.

Proskauer - Blockchain and the Law. Blockchain 51% Attacks – Lessons Learned for Developers and Trading Platform Operators. https://www.jdsupra.com/legalnews/blockchain-51-attacks-lessonslearned-25298/, 2020. [Online February 13, 2020].

PTI. EC with IIT-Madras to explore blockchain technology for voting. https://government.economictimes.indiatimes.com/news/digital-india/ec-with-iit-madras-to-exploreblockchain-technology-for-voting/74161191, 2020. [Online February 20, 2020].

PTI. E-voting to become reality soon? EC working with IIT-M on Blockchain Technology. https://www.livemint.com/elections/assembly-elections/evoting-to-become-realitysoon-ec-working-with-iit-m-on-blockchain-technology-11616755074358.html, 2021a. [Online March 26, 2021].

PTI. CEC Says Mock Trials for Blockchain-Aided 'Remote Voting' to Begin Soon. https://thewire.in/ government/election-commission-national-voters-day-remote-voting, 2021b. [Online January 25, 2021].

Harshit Rakheja. India Explores Blockchain-Based E-Voting By 2024 General Elections. https://inc42. com/buzz/india-explores-blockchain-based-e-voting-by-2024-general-elections/, 2021. [Online March 27, 2021].

Ronald L. Rivest. Electronic Voting. https://people.csail.mit.edu/rivest/RivestElectronicVoting.pdf, 2001. [Accessed April 29, 2019].

Ronald L. Rivest. On the notion of software independence in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767, 2008. doi:10.1098/rsta.2008.0149. https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2008. 0149.

Zeynep Tufekci. Online Voting Seems like a Great Idea - Until You Look Closer. *Scientific American*, 2019. https://www.scientificamerican.com/article/online-voting-seems-like-a-greatidea-until-you-look-closer/?redirect=1 [Online June 1, 2019].

Appendix: Construction of an append-only public bulletin board

The construction of a public bulletin board consisting a sequence of bulletins $<B_1,B_2,...,B_n>$ is based on two technical concepts from computer science:

1. ***Digital signature:*** The digital signature s = **sign**(msg,sk) of a message *msg* is signed using a publicly known function **sign** and a secret key *sk*, and it can be verified using a publicly known function **verify**(msg,s,pk) which returns either *true* or *false*, using the public key *pk* of the signing authority. A digital signature is non-repudiable and the signature and the integrity of the message can be publicly verified by anybody using the pre-published public key of the signer.
2. ***Hash function*:** A hash $h = H(msg)$ of a message *msg* is computed using a publicly known hash function H. A hash function has two main properties. It is *one-way*, i.e., given a hash value h it is computationally difficult (intractable) to find a *msg* such that $h = H(msg)$; and is *collision resistant*, i.e., finding msg_1 and msg_2 such that $H(msg_1) = H(msg_2)$ is computationally difficult. The above two properties guarantee that once the hash of a message is published, it becomes practically impossible to alter the message.

Using the above, a public bulletin board may be realised by requiring that for each bulletin B_i

$B_i = (m_i,T_i,W_i,h_i,WSign_i,BSign_i)$

where m_i is the message of the bulletin and must contain a searchable reference to an issued receipt or a commitment, T_i is the writer's timestamp, W_i is the identity of the writer (the sub-authority of ECI that is posting the message), h_i is a hash computed by any suitable publicly committed cryptographically secure one-way and collision resistant hash function H, $WSign_i$ and $BSign_i$ are signed terms as described below. The bulletins must satisfy the following *invariant*:

1. $h_i = H(m_i \cdot T_i \cdot W_i \cdot h_{i?1})$; where $h_0 = 0$ and $\cdot$ is the string concatenation operator.
2. $WSign_i = SW_i(h_i)$; where $SW_i()$ indicates signing with the private key of the writer.
3. $BSign_i = SB_i(WSign_i.T'_i)$; where $SB_i()$ indicates signing with the private key of the bulletin board, and Image not found or type is the bulletin board's timestamp at the time of signing, which must be within a bounded small delay after the writer's timestamp.

The above will have protection against insertion, deletion and alteration of messages even if the writers and the bulletin board collude (Heather and Lundin, 2009). If the writer and the bulletin board maintainer are the same authority (not recommended; the bulletin board may be maintained by an independent agency, or even multiple independent agencies) then it will be necessary for some readers to read whenever there is an update (or at least once in a while), or for the bulletin board to push out (upload) the differential bulletin board content to some neutral place. Concurrency control for multiple writers may be realised by serializing using standard distributed computing protocols.

The requirements outlined above constitute a special case where all writing authorities are sub-jurisdictions of the ECI and there is no possibility of any conflict in the time order of writing records, and the requirements of precise timing of reading and writing are somewhat relaxed.