E-Voting is a problem with many difficulties. Many of the desired e-Voting properties have trade-offs. On one hand, for example, privacy is a main requirement as votes should be anonymous to prevent coercion. On the other hand, evoting should provide some sort of public verifiability, because otherwise, the provider of the e-voting solution – or someone who managed to compromise it – might be able to change votes at will. In e-voting, many parties are involved and these parties typically do not trust each other.

At the same time, evoting systems require public verifiability, and thus, many have proposed to base e-voting systems on blockchain technology. Due to the requirements, it seems reasonable that blockchain technology can help to achieve some of the desired properties. However, to the best of our knowledge, so far, no solution has been proposed that has been shown to be secure, verifiable, and private and there are still many open challenges. Following our methodology – and depending on the trust model – one could use an always online trusted third party, as is the case in today’s e-voting systems. However, it is possible that the state is trusted for voter registration but not for recording and tallying the votes of the election or referendum.

In this case, we have an offline trusted third party, i.e. a public 52 permissioned blockchain may be a good fit. Such a system could be designed as a permissioned blockchain in which political parties, NGOs or other partially trusted organizations could take roles as validators. The security depends on the distribution of the validators, however, and one must be careful with assigning these roles. If, for example, a system assigns validator roles proportionally to the strengths of parties in the last election, no additional properties in terms of trust is gained, if a single party has a majority

If a trusted third party (TTP) is available, there are two options. First, if the TTP is always online, write operations can be delegated to it and it can function as verifier for state transitions. Second, if the TTP is usually offline, it can function as a certificate authority in the setting of a permissioned blockchain, i.e. where all writers of the system are known. If the writers all mutually trust each other, i.e. they assume that no participant is malicious, a database with shared write access is likely the best solution. If they do not trust each other, using a permissioned blockchain makes sense. Depending on whether public verifiability is required, anyone can be allowed to read the state (public permissioned blockchain) or the set of readers may also be restricted (private permissioned blockchain). If the set of writers is not fixed and known to the participants, as is the case for many cryptocurrencies such as Bitcoin, a permissionless blockchain is a suitable solution [1]

Why not Internet voting (vote from home)?

* [Duncan Buell](https://electionverification.org/aee-blockchain/), a computer science professor at the University of South Carolina who focuses on voting systems and election integrity, has been strongly opposed to digital voting from as far [back as 2015](http://www.thestate.com/opinion/op-ed/article16523588.html) and feels like this new idea of blockchain voting brings in too many issues.
* “I am strongly opposed to electronic voting, and I think the whole notion of internet voting is completely nuts,” [Buell says](https://statescoop.com/meet-the-guy-paying-for-west-virginia-to-run-an-election-on-blockchain).
* *“There are a number of issues that come up. The first is authentication. How do you verify who’s at the other end?”*
* He is more referring to the company, Voatz, which ran the election here and their protocols which include fingerprint-scanning or facial-recognition technology on its users' smartphones, but Buell maintains these can be hacked.

There is a trade-off between the throughput and security of blockchain systems,

Since real-world implementation with thousands of nodes is extremely challenging in many cases. Recent studies on blockchain systems suggest that there is a trade-off between the performance and security of PoW-based blockchains. Due to the tradeoff, it is imperative to study the security concerns of blockchain voting systems.

## What does blockchain offer?

* The interest in blockchain technology taking over from traditional election methods has potential advantages due to the big technological upgrade from how elections are currently held. Many national elections still take place using a paper-based system, leaving open huge holes for [security](https://cointelegraph.com/tags/security) breaches, [fraud](https://cointelegraph.com/tags/fraud), and [corruption](https://cointelegraph.com/tags/corruption).
* Blockchain offers an updated system for voters that could potentially fix these concerns.
* Its traditional assets, such as its [transparency](https://cointelegraph.com/news/blockchain-based-secure-online-voting-system-showcased), allow for votes to be followed, counted, and correlated by many different sources while still maintaining the privacy of the voters due to the anonymous transactions along the blockchain.
* We thought of an online voting in which everyone would be able to vote from there homes , but as Duncan Buell says, we don’t know who is at the other end, and many people are still used to driving to polling stations , so we just made a blend of the old method with the internet voting i.e bla bla bla which is going to make it more comfortable for people to adapt.

**Title**

DE-Vote

**Name of Supervisor**

Professor Dr. Moazzam Jawed

**Introduction**

* Elections have been subject to scrutiny and corruption for so long that many in the tech space, as well as electoral committees are viewing blockchain as the future of fair elections.
* There have been some [use-cases already](https://cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections) where blockchain has come to the aid of elections. Different countries and organizations have begun experimenting with the immutable distributed ledger that offers transparency and security.

**Related work**

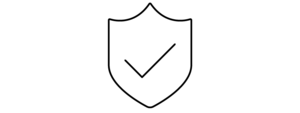
* On March 7, it was reported as an apparent world-first that [Sierra Leone has employed blockchain technology](https://cointelegraph.com/news/sierra-leone-uses-blockchain-to-track-election-results-swiss-company-provides-expertise)
* West Virginia's primary election on May 8 seeing the [completion of the first government-run, blockchain-supported](https://cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections)vote in US history.( Again, this was not a full blockchain election, as it was only available to a select group of voters, such as military members.)
* The [South Korean](https://cointelegraph.com/tags/south-korea) government is considering using [blockchain](https://cointelegraph.com/tags/blockchain) technology for an electronic voting system, business technology news website [ZDNet](https://www.zdnet.com/article/south-korea-to-develop-blockchain-voting-system/#ftag=RSSbaffb68) and CoinTelegraph reports Nov. 28. [2]

**Problem statement**

The voting systems that have been utilized globally to permit people cast their ballots are either paper-based (conventional) or electronic-based. Not only using paper ballots and counting them is prone to errors but also is a time-consuming process. However, the risks of the E voting (Centralized) is so substantial and the cost of any interference with an e-voting system is beyond fatal. All in all, the existing voting systems, whether they are electronic or conventional, involve insufficient levels of transparency since the election data is under control of a third party. In effect, in either case it becomes extremely difficult or unbearable for voters to ensure that their election votes are counted carefully and accurately by the election administrators.

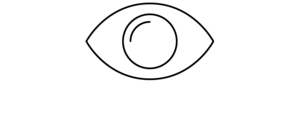
**Aims and Objectives**

* Our aim is to develop a Decentralized E-Voting System using Blockchain for conducting elections
* Our objective is to develop such blockchain for our E-Voting system that can process a lot more transactions than the other blockchains (e.g. Bitcoin, Ethereum etc.)
* Such system that provides a substantial level of transparency by sustaining an exposed registry of votes, while defending the privacy of the voters.
* To develop such a system that is tamper proof (no single entity has control over the election data), the TP’s only role would be deployment of the system.
* To make elections less costly
* To reduce the amount of time, work and HR required



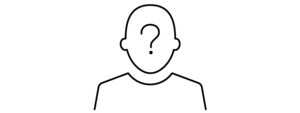
**TAMPER-PROOF**

Ballots and results cannot be altered by any third party.



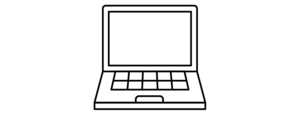
**TRANSPARENT**

The entire voting process is fully transparent and publicly verifiable.



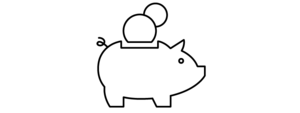
**PRIVATE**

Voters’ choices and identities are protected.



**ACCESSIBLE**

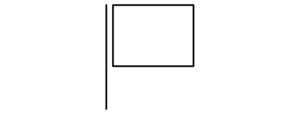
Voters can participate in a modern, convenient and fair way.



**AFFORDABLE**

Digitization of paper and manual processes reduces election costs. According to Dawn This year’s general elections cost over 21 bn Rs.

* Secretary Election Commission of Pakistan (ECP) Babar Yaqoob Malik has said that the printing process of some 220 million ballot papers has begun under the supervision of Pak army which would be completed till 20th July
* Plus the plastic waste is also insane.
* ECP set approximately 85000 polling stations in this years elections, if one device for one polling station costs 25000 than the total cost won’t exceed 3 bn, look how much we can save, and these devices are just one time investment.

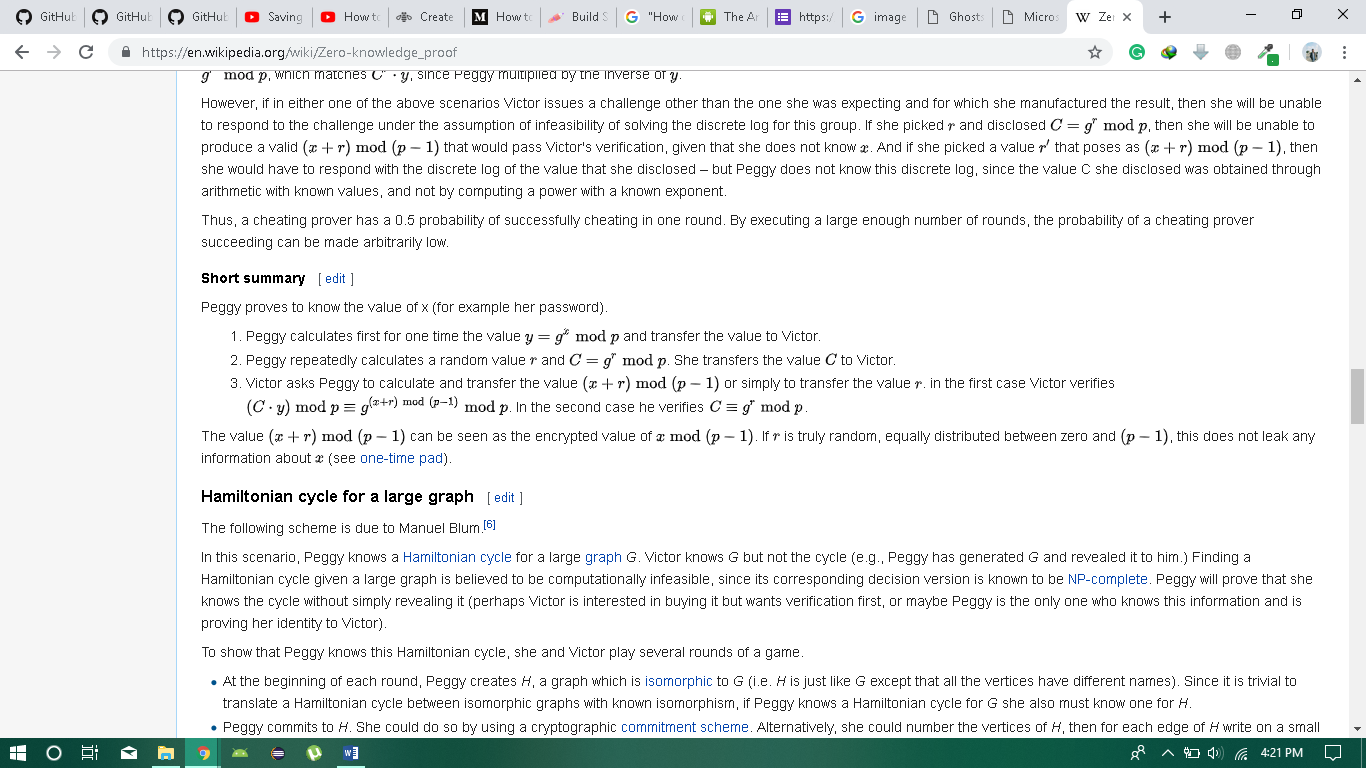


**TENSION-LESS**

Eliminating violence caused by questionable results.

**Methodology:**

Zero knowledge proof:



BFT (Byzantine Fault Tolerance)

Proof of Vote

ElGamal/Paillier Cryptosystem (Homomorphic Encryption)

Homomorphism feature allows one to operate on ciphertexts without decrypting them [11]. For a voting system, this property allows the encrypted ballots to be counted by any third party without leaking any information in the ballot

Permissioned Blockchain:

available for everyone to read, but don’t allow anyone to be a node, serving the network’s security, transaction verification or mining.

**Proposed tools**

Blockchain, Biometric Fingerprint Scanner, Python, HTML, CSS, Flutter, React native, Adobe Illustrator (for designing)

**Proposed Outcomes**

A fully functional blockchain based decentralized e-voting platform for conducting any kind of elections from small to a very large scale.

**References**

Agora and Polys White Paper and other research papers.

Building Secure Elections [3]

A Survey of Different Electronic [4]

Blockchain Based E-Voting Recording [5]

Agora [6]

[6] Mulcair handed NDP reins; Successor to Layton faces big challenges". Calgary Herald, March 25, 2012.

[7] Michael Safi. "NSW election result could be challenged over iVote security flaw". The Guardian. Archived from the original on 2016-11-24.

Bitcoin is built using Blockchain [7]

# References

|  |  |
| --- | --- |
| [1] | K. Wüst, "Do you need a Blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology*, 2018. |
| [2] | M. Yakubowski, "cointelegraph.com," Coin Telegraph, 28 11 2018. [Online]. Available: https://cointelegraph.com/news/south-korean-government-to-test-blockchain-use-for-e-voting-system. [Accessed 28 11 2018]. |
| [3] | D. P. Moynihan, "Building Secure Elections: E‐Voting, Security, and Systems Theory," *Public Administration Review,* vol. 64, no. 5, pp. 515-528, 2004. |
| [4] | A. M. A. HTET NE OO, "A Survey of Different Electronic Voting Systems," *International Journal of Scientific Engineering and Technology Research,* vol. 3, no. 16, pp. 3460-2464, 2014. |
| [5] | B. R. Rifa Hanifatunnisa, "Blockchain Based E-Voting Recording System," in *11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Lombok, 2017. |
| [6] | M. V. Rubtcova and O. V. Pavenkov, "Implementation of Blockchain Technology in Electronic Election in Sierra Leone," , 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3147252. [Accessed 4 12 2018]. |
| [7] | B. Marr, "forbes.com," forbes, 16 02 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#6e81ced47bc4. [Accessed 04 12 2018]. |

The existing voting systems, conventional or electronic, involve insufficient levels of transparency since the election data is under control of a third party which makes it extremely difficult for voters to ensure that their election votes are counted carefully and accurately by the election administrators.