Blockchain-based Voting Systems for university elections

1 Introduction

Electoral voting for student government is an essential democratic process of universities, yet issues of voter transparency and security remain. In this review, we analyse the advantages and disadvantages of currently applied manual and e-voting schemes and assess several proposed blockchain-based voting systems in the literature. Finally, we present a voting system for a university-wide application that implements blockchain to improve transparency and security concerns.

2 Manual and Electronic Voting Systems

Current voting protocols at the University of Sydney may either take on manual or electronic voting modes.

Manual Voting

Manual voting, where voters cast their vote at designated and supervised locations and where election officials aggregate votes by hand, poses several disadvantages for voters and administrators. For voters, availability to vote is restricted to set times and there is a lack of transparency that their vote was correctly counted and included. For administrators, vote aggregation can be an arduous task that is prone to tallying errors and poor record keeping. Examples of documented manual voting errors are those of the 2005 parliamentary elections of Germany as described by Meter [1]. In one case, initial tallying of votes in the Bochum-Langendreer district resulted in 491 of 689 votes marked as invalid. After a re-tally of votes, only 13 ballots were marked invalid. This re-tallying resulted in a win for a different party than what was initially reported [1]. Although this parliamentary example differs from our University scope, it highlights the potentiality of human errors on the voting process which may reduce voters' trust towards the system. Another disadvantage of traditional paper voting is that it requires costly resources (e.g. paper materials, staff) over the course of the voting process [1].

Given these shortcomings of high cost, error-proneness and lack of transparency, improvements can be made to increase the efficiency of the manual voting process.

E-voting

Electronic voting (e-voting) can be viewed as an optimisation over the manual voting method to reduce human error and increase voter convenience, however, the technology introduces its own set of drawbacks. We define an e-voting system as using the internet and cryptographic protocols to realise an election, in which eligible voters vote using their own device [1].

The benefits of e-voting include the perceived increase in voter convenience, by transforming the voting task to be on par with the cost of checking an email or going online [2]. The effect to which voters find more convenience with e-voting still remains unclear and is often studied with respect to voter turnout. For example, a time-series study on state elections of Ontario between 2000 and 2014 showed that adoption of e-voting systems increased voter turnout by 3.5% over time [2]. In another study in Switzerland, the introduction of postal voting saw an increase of 4.1% in voter turnout, however, when e-voting was introduced researchers found no additional effect on turnout [3]. Therefore, convenience may vary depending on other factors such as attitudes and preferences of voters.

A better-understood benefit of e-voting is its reduced cost in administration. e-voting can be implemented to reduce resource costs and minimise staff provisioning and paper materials [4]. Furthermore, the automation of vote tallying reduces human errors and speeds up the counting process [4].

Hesitations against e-voting lie in the concerns of the system to successfully maintain voter anonymity, the accuracy of votes, security and prevention of fraud. Previous parliamentary e-voting systems include the Estonian I-Voting, Norwegian I-Voting, NSW iVote system and the D.C Digital Vote-by-Mail Service [1, 5]. These systems have been evaluated in the literature, with underlying problems shown to be a failure of providing total anonymity or integrity, proneness to DDoS attacks because of their centralisation and lack of transparency from the programming code [5].

Challenging the security mechanisms of theoretical and applied e-voting systems is warranted to question strong assumptions for these systems (e.g. assumptions of voters device security, assumption of the integrity of non-publicly available code). These underlying problems suggest that poor implementations of e-voting systems can function as no-better than manual voting.

For the University's case, information on the e-voting systems and protocols are not made publicly available. Based on the most recent Student Fellows of Senate election, voting was performed under proprietary software owned by BigPulse. This appears to be a disadvantage for voters as it introduces yet another problem of lack of transparency and vote secrecy.

For University clubs and societies' board committee elections, there is no common voting platform. Most committees use paper ballots for voting, which is time-consuming, untransparent and inconvenient, thus the number of voters is not high. For example, the voter turnout for SUPRA (Sydney University Postgraduate Representative Association) General Election 2018 was only close to 1,500, while the number of eligible voters was more than 25,000 (6%) [6].

3 Distributed Approach

Researchers have proposed the application of blockchain technology to improve the voting process. Blockchain, first introduced by Nakamoto in 2008 [7], has garnered considerable interest in improving upon past e-voting systems in terms of transparency and security. Furthermore, the use of smart contracts will be discussed as a way to incorporate self-enforcing protocols within the blockchain to increase autonomy.

3.1 Blockchain

A blockchain scheme of the voting process relies on publicly verifiable time-based ordered blocks to store ballots and/or voting results. Blocks are distributed to store the complete database and each new block appended to the chain has been verified through a consensus protocol. It is difficult to modify old values in the chain as all following blocks will have to be recalculated which is infeasible due to its computational expense [8].
As described by Vukolic [9], there are two typical approaches in achieving consensus:
Proof-of-Work (PoW) protocol: In PoW-based blockchains, node identities are entirely de-centralised, meaning that nodes do not need to know the ID of other nodes.
Practical Byzantine Fault Tolerance (PBFT) protocol: In BFT-based blockchains, nodes are permissioned such that it requires every node to know the identity of its peer nodes participating in consensus. Therefore, a trusted authority must issue identities and cryptographic certificates to nodes.

The advantage of PoW over PBFT is its high scalability of the number of nodes and decentralised identity management. BFT has its advantages of less network latency due to satisfying the requirement of consensus finality. This means that the final inclusion of a transaction into the blockchain can be immediately confirmed. Generally, consensus protocols are what makes the blockchain publicly verifiable and improves the transparency of data being stored as nodes have to agree on the order of the blocks. The distributed infrastructure and decentralised actors can improve upon the weaknesses of centralisation as seen in past e-voting systems.

3.2 Smart Contracts

Smart contracts are scripts stored on the blockchain that can autonomously and automatically execute on every node in the network. These scripts can be expressive functions that execute predefined and deterministic protocols between entities in the network, which are enacted by addressing a transaction to its location [8]. Smart contracts can also be used to allow end users to create and query data on the blockchain [10]. Since it is stored on the blockchain, everyone on the network can inspect the code and trace the contract's operations [8]. An example of smart contract usage in a voting system is described in McCorry et al.'s Open Vote Network on the Ethereum platform: They crafted a smart contract that required each eligible voter to deposit ether upon registration and to automatically refund the ether when their vote was accepted in the blockchain. A self-tallying protocol was also implemented to count all the casted votes [11]. Smart contracts thus operate as *autonomous actors* within the network [8], allowing developers to go beyond explicit data storage and incorporate general self-executing computations but more powerfully, self-enforcing protocols between network participants.

4 Blockchain-based voting systems

As described by Yu et al. [10], blockchain implementations of voting systems can fall under three broad categories:

Voting systems using cryptocurrency: In [12], Bistarelli et al. proposed an end-to-end e-voting system based on Bitcoin where eligible voters can directly cast a vote on the blockchain. The drawback of their approach is the uncertainty of data confidentiality. Once a casted vote is broadcasted on the network, the candidate's address can be read and may affect successive votes.

In [13], Takabatake et al. proposed an e-voting system using Zerocoin to address the lack of assurance Bitcoin provides for complete voter anonymity. Zerocoin acts as an additional layer to conceal the voters' identities while at the same time retaining eligibility and verifiability. A drawback of these cryptocurrency approaches is that voting protocols must be externally and actively enforced by the voters themselves.

Voting systems using smart contracts: In [11], McCorry et al. presented the first implementation of a fully independent and decentralised voting system using blockchain for self-tallying and privacy protection using smart contracts. Similar to [12], there exists an *adaptive issue* meaning the tally so far can affect how the last voter places her vote. Furthermore, a voter can abort the election without casting their vote which prevents all other voters from computing the final tally. The limitation of 50 voters makes it impractical for our University-wide application [10]. In [10], Yu et al. presented a platform-independent system using smart contracts which do not require the voter to trigger the tallying phase. This handles the abortive issues from [11], as voters can quit before an election ends without affecting the tallying of ballots.

Voting systems using blockchain as a ballot box: Commercial voting systems such as FollowMyVote and Tivi use blockchain as a ballot box from which a central authority decouples a voter's identity from their voter key to achieve voter privacy [10, 11]. However, voter's privacy is hard to evaluate and authority can be compromised.

4.1 Evaluation

After analysis of blockchain-based voting systems in Section 4, we compare the approaches in terms of our university application. We suspect that using blockchain as a ballot box does offer improvements in vote record keeping and consistency but it still has issues of centralisation and lack of transparency. Alternatively, using cryptocurrency, the voters themselves must enforce the protocols which may pose a higher cost of participation for both voters and administrators of the network that may translate to an inconvenience. Using smart contracts allows for self-executing protocols such as autonomous tallying and end user interaction which supports decentralisation of authority and automation of aspects of the voting process. Between the systems using smart contracts, we found that the platform-independent scheme proposed by Yu et al. [10] provides the most benefits in terms of scalability and flexibility for our university application as the tallying process does not require the participation of all eligible voters.

5 Knowledge Gaps

With respect to the voting systems discussed in Section 4, we highlight the knowledge gaps based on the existing literature:

Voter Device Security: Strong assumption that voters' devices are secure.

Coercion Analysis: Coercion is the act of a coercer forcing another person to vote for a specific candidate. Ideally, a voting system should have security mechanisms in place to reduce acts of coercion. Realistically, a completely coercion-resistant system may not ever be achieved[1]. Acts of coercion are hard to validate, for example measuring that a voter's vote is due to personal intention or dependent on a coercer is intangible. While it has been argued that the University student demographic is an example of a low-coercion environment compared to high-stakes parliamentary elections [14], blockchain-based voting systems are still in its infancy with regards to real-world applicability in high-coercion environments.

Insider Attacks: Blockchain implementations still rely on granting a higher level of trust to voter administrators to not disclose information on cryptographic keys and special permissions of ballot decryption. This introduces the possibility of compliance breaches of insiders with adversarial motives. One way to mitigate this issue is to grant different levels of permissions amongst administrators [1], however, such attacks still remain an open issue that needs to be considered when assessing risk factors.

Voter Usability: Usability analysis is critical for the widespread adoption of a system. While there has been research on the usability of past e-voting systems [1], the usability of the blockchain systems in Section 4 has not been analysed in depth.

Effect on Voter Turnout: In Section 2 we introduced conflicting evidence regarding the effect of e-voting adoption on voter turnout. To our knowledge, research regarding the effect of blockchain schemes for votings systems and its effect on perceived user trust and voter turnout is yet to be explored.

6 Proposed solution

For the development of the blockchain-based voting system for university elections, we have employed the platform-independent voting system using the PBFT consensus protocol proposed by Yu et al. [10], with a slight modification. Our contribution focuses on improving *voter usability* of blockchain-based voting systems. This involves a re-working of the registration process by making use of the existing University student database. Voter verification is derived from the student database and registration will be simplified to a voter logging in with their student credentials through a web application. For this to work, we propose a voting distributed application (Dapp) with smart contract functionalities on the Ethereum platform accessible via a web browser with support from the MetaMask extension, which allows users to interact with the blockchain without actually having to set up a node. The platform design is shown in Figure 1.

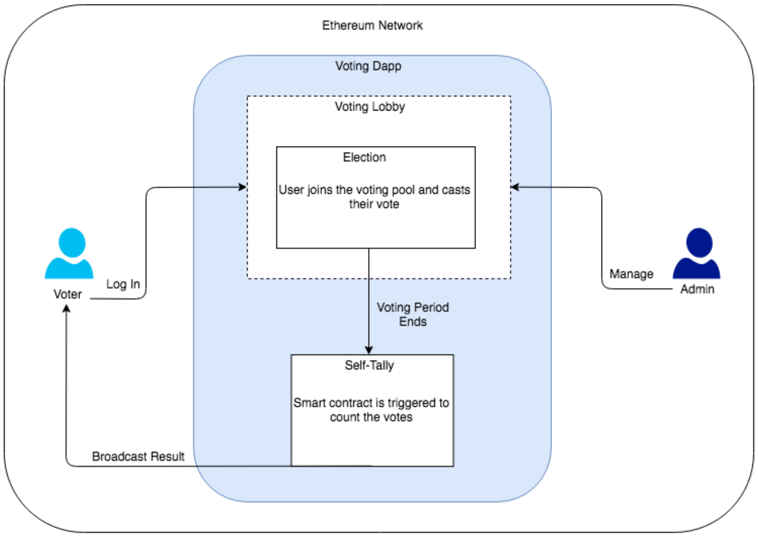

Figure 1: Platform design on the Ethereum Network

Our system involves three actors: the voter, smart contracts and the administrator and is displayed in Figure 2. We adopt the same security measures proposed by Yu et al. [10]:
Homomorphic Encryption: This feature allows a third party (i.e. the administrator) to count encrypted ballots without leaking any information in the ballot.
Linkable Ring Signature: Linkable Ring Signature allows anyone to determine that a voter has only voted once, while still preserving voter anonymity.
Proof of Knowledge: This mechanism is employed so that a voter can prove they know their ballot contains one legitimate candidate which asserts the validity of their ballot, without revealing candidate information.

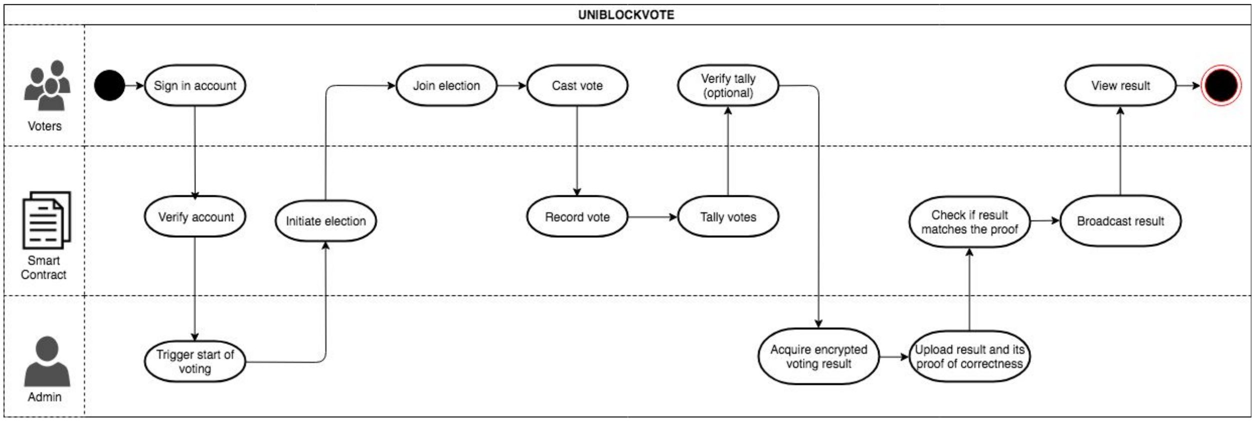

Figure 2: Voting Protocol diagram of *UniBlockVote*

6.1 Consolidation

Comparison of our solution compared to manual and e-voting is shown in Table 1. Using blockchain we have exploited a high level of decentralisation, a feature that supports the transparency and security of the voting process for voters and administrators alike. Additionally, the benefit of low cost and manpower of e-voting systems is retained compared to manual voting. However, the level of coercion-resistance remains equivalent to e-voting.

	Manual Voting	E-voting	Blockchain Voting
Cost/Manpower	High	Low	Low
Transparency	Low	Medium	High
Coercion-Resistance	High	Medium	Medium
Security	Medium	Medium	High
Decentralisation	Low	Low - Medium	High

Table 1: Comparison of manual, e-voting and blockchain voting

7 Conclusion

In this review, we introduced a blockchain-based voting system that uses smart contracts to enable a secure and transparent election while still maintaining cost efficiency. By comparison to previous work, our contribution of improving voter usability of blockchain-based schemes prioritises voter participation and turnout, allowing for its suitability for university-wide student elections.

References

1. Meter C. Design of Distributed Voting Systems. 2017. In: arXiv:1702.02566.
2. Alvarez M, Levin I, Li Y. Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. Journal of Information Technology & Politics. 2018; 15 (2): 94-105.
3. Luechinger S, Rosinger M, Stutzer A. The Impact of Postal Voting on Participation: Evidence for Switzerland. Swiss Political Science Review 2007;13 (2):167–202.
4. Kumar S, Walia E. Analysis of Electronic voting systems in various countries. IJCSE. 2011; 3 (5): 1825-1830.
5. Ayed, AB. A Conceptual Secure Blockchain Based Electronic Voting System. International Journal Of Network Security & Its Applications. 2017; 9 (3): 1-9.
6. Sydney University Postgraduate Representative Association. SUPRA 2018 Annual Report. Sydney NSW: SUPRA; 2018. Available from: http://www.supra.net.au/wp-content/uploads/2018/05/Annual-report-2018_web-version.pdf
7. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available from: http://www.bitcoin.org/bitcoin.pdf
8. Christidis K, Devetsikiotis. Blockchain and Smart Contracts for the Internet of Things. IEEE Access. 2016; 4: 2292-2303.
9. Vukolic M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In:
   Proceedings of the IFIP WG 11.4 Workshop iNetSec 2015.
10. Yu B, Liu J, Sakzad A, Nepal S, Steinfeld R, Rimba P, Au MH. Platform-independent Secure Blockchain-Based Voting System. In: Chen L, Manulis M, Schneider S. (eds) Information Security. ISC 2018. Lecture Notes in Computer Science, vol 11060. Springer, Cham.
11. McCorry P, Shahandashti SF, Hao F. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. In: Kiayias A. (eds) Financial Cryptography and Data Security. 2017; 357-375.
12. Bistarelli S, Mantilacci M, Santancini P, Santini F. An end-to-end voting system based on bitcoin. In: Seffah A, Penzenstadler B, Alves C, Peng X. (eds) Proceedings of the Symposium on Applied Computing. SAC 2017. Marrakech, Morocco 2017; 1836–1841.
13. Takabatake Y, Kotani D, Okabe Y. An anonymous distributed electronic voting system using Zerocoin. IEICE Technical Report. 2016; 116 (282): 127-131.
14. Adida B. Helios: web based open-audit voting. In: Proceedings of the 17th conference on Security symposium. SS 2018. Berkeley, CA, USA 2018: 335–348. USENIX Association.