

UDC 519.6
DOI <https://doi.org/10.26661/2413-6549-2021-2-06>

USING BLOCKCHAIN TECHNOLOGY IN VOTING

Kolesnikov V. A.

Ph.D., Professor at the Department of Computer Science

Sumy State University

Rymaskogo-Korsakova str., 2, Sumy, Ukraine

orcid.org/0000-0002-1991-3614

v.kolesnikov@cs.sumdu.edu.ua

Key words: *blockchain, Smart Contracts, election, Web application.*

This paper discusses blockchain technology and its associated tools, considers the application of this technology, presents a Web application for voting in elections as an example of the application and discusses advantages and disadvantages of blockchain technology in general and in regard to voting in particular. Blockchain technology was developed for first cryptocurrency known as Bitcoin as its transaction mechanism. It is decentralized in nature and nowadays found its place in many areas including financial and insurance markets. The technology allows to validate user entries, safeguard them preventing the possibility of a change, preserve them for historic purposes and secure against unauthorized access due to its decentralized nature. Users have full access to their records at all times. Information is reliable and up-to-date. When a transaction record is created, all necessary information about the transaction is created and placed in there and public key – private key mechanism is employed. The transaction record is then broadcast to every party in the network, verified and recorded in the public ledger. Blockchain technology can be utilized in voting. Conventional voting systems are usually centralized. That poses security and efficiency limitations. Electoral fraud is another issue in elections and results in lower voter turnout that in turn makes it easier to commit fraud. Fairness is a big aspect in elections in many countries. The characteristics of blockchain technology mentioned above nicely fit for this purpose. We developed a voting Web application as a proof of concept. Instead of money as in the case with cryptocurrency we use a single vote as a digital asset transaction. Validation, safeguarding and preservation of entries are all needed in voting and will be guaranteed by the blockchain technology. Our application is designed as a decentralized Web voting system, which provides a public and transparent voting process while protecting the anonymity of voter's identity, the privacy of data transmission and verifiability of ballots. We also consider current limitations of the technology related to voting. Some major disadvantages of using a blockchain technology are access to a computing device and required technological maturity. These problems might exclude some population from voting. A natural solution is to use a mixed approach wherein paper ballots are provided as a backup on a few polling stations. Nevertheless, blockchain technology is appropriate for using as an election mechanism, which was showcased as a proof of concept in this paper.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ BLOCKCHAIN У ГОЛОСУВАННІ

Колесніков В. А.

*Ph.D., професор кафедри комп'ютерних наук
Сумський державний університет
вул. Римського-Корсакова 2, Суми, Україна
orcid.org/0000-0002-1991-3614
v.kolesnikov@cs.sumdu.edu.ua*

Ключові слова: *blockchain, Smart Contracts, вибори, веб-додаток.*

У роботі обговорюється технологія blockchain та пов'язані з цією технологією інструменти, розглядається застосування цієї технології, представлено веб-додаток для голосування на виборах як приклад застосування технології та обговорюються переваги та недоліки технології blockchain загалом та стосовно голосування зокрема. Технологія blockchain була розроблена для першої криптовалюти, відомої як Bitcoin, як механізм транзакцій. Ця технологія має децентралізований характер і сьогодні знайшла своє застосування у багатьох сферах, включаючи фінансовий та страховий ринки. Технологія blockchain дозволяє перевіряти записи користувачів, захищати їх, запобігаючи можливості зміни, зберігати їх для історичних рекордів та захищати ці записи від несанкціонованого доступу через її децентралізовану природу. Користувачі завжди мають повний доступ до своїх записів транзакцій. Інформація достовірна та актуальна. Коли створюється запис транзакції, вся необхідна інформація про транзакцію розміщується в рекорді, а також використовується механізм публічного ключа – приватного ключа. Потім запис транзакції передається кожній стороні в мережі, перевіряється та записується в публічну книгу записів. Технологію blockchain можна використовувати при голосуванні. Системи голосування зазвичай є централізованими. Це обмежує безпеку та ефективність. Шахрайство на виборах – це ще одна проблема на виборах, що призводить до зниження явки виборців, що, в свою чергу, полегшує вчинення шахрайства. Прозорість – це важлива і бажана характеристика виборів у багатьох країнах. Згадані вище характеристики технології blockchain добре підходять для цієї мети. Ми розробили веб-додаток для голосування як доказ концепції. Замість грошей, як у випадку з криптовалютою, ми використовуємо один голос як транзакцію цифрового активу. Перевірка та збереження записів, необхідні під час голосування, гарантовані технологією blockchain. Наш додаток розроблений як децентралізована система веб-голосування, яка забезпечує публічний та прозорий процес голосування, захищаючи при цьому анонімність особи виборця, конфіденційність передачі даних та можливість перевірки бюлетенів. Ми також враховуємо поточні обмеження технології, пов'язані з голосуванням. Деякі основні недоліки використання технології blockchain – це доступ до обчислювального пристрою та необхідна технологічна зрілість. Ці проблеми можуть виключити частину населення від голосування. Природним рішенням є використання змішаного підходу, за якого паперові бюлетені надаються як резервні на кількох виборчих дільницях. Тим не менш, технологія blockchain є доцільною у використанні як механізм виборів, що було продемонстровано як доказ концепції в цій роботі.

1. Introduction

Blockchain is a decentralized transaction and data management technology that today is revolutionizing many areas [1–3]. It was first developed for Bitcoin cryptocurrency transactions in 2008 and hence cemented its place in the financial sector [1].

Blockchain technology is also used in insurance, notary public and even music industry [1–2]. In this paper we discuss the strong sides of blockchain technology, apply it to voting and present a voting web application based on the technology, and finally consider the current limitations of the technology

in general and those limitations that are specific to voting in particular.

A review of blockchain-based voting systems has been performed in recent years [4–10]. For example, a classification of blockchain voting systems was performed based on the types of blockchain used, the consensus approaches used, and the scale of participants. In our approach, we surveyed existing blockchain technologies and its tools, selected the minimum set of such instruments, and applied them to the problem of voting.

2. Blockchain technology

We will briefly describe the blockchain technology using a financial example presented in Fig. 1. At the same time, we note that this technology is applicable to any digital asset transaction. In the scenario shown in Fig. 1 Alice wants to transfer some money to Bob. Alice initiates the transfer. A transaction record known as a “Block” with all necessary information about the transaction is created using public key – private key mechanism. The transaction record is then broadcast to every party in the network, verified and recorded in the public ledger. The verification step ensures that the sender owns the money and that the sender has sufficient amount in his account. The transaction is finalized and the money is transferred.

Next, we list advantages of blockchain technology:

- Validation of entries.
- Safeguarding of entries (transactions cannot be changed).

- Preservation of historic records (transactions cannot be deleted, users have access to the history of transactions).

- Decentralized nature (not connected to a centralized database).

- Users have full access to and control over their data.

- Reliable and up-to-date data.

- It can withstand and repel unauthorized access due to its decentralized nature.

- Difficult to hack due to its decentralized nature.

- No central authority is needed to verify transactions.

These advantages make the blockchain technology applicable to and desirable for many areas. We consider next the problem of fair voting and the application of this technology to the area of voting.

3. Application of blockchain technology to voting

3.1. The problem of voting

People often express their opinion or choice through voting. For example, in many countries presidents are elected by the country’s citizens through voting. Presidents of academic universities or academic department chairs are also often selected according to the results of voting by appropriate constituents. Conventional voting systems are usually centralized. That poses security and efficiency limitations. Electoral fraud is another issue in elections and results in lower voter turnout that in turn makes it easier to

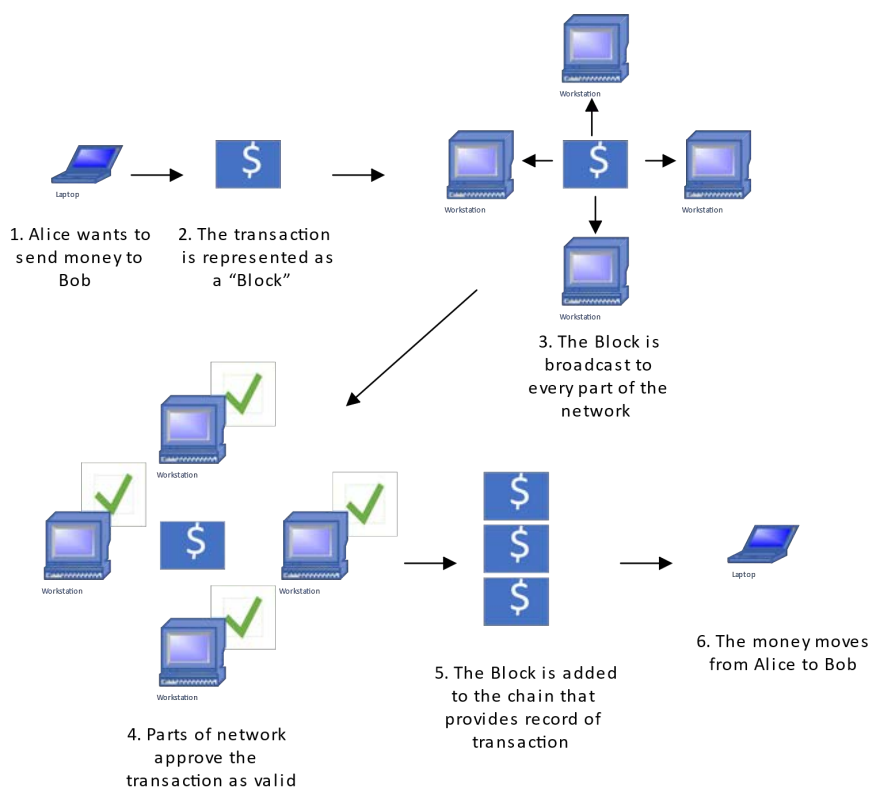


Fig. 1. Blockchain technology

commit fraud. Fairness is a big aspect in elections in many countries. Hence, there has been a trend of moving to decentralized voting systems. Blockchain technology seem to fit nicely here as a solution.

3.2. Application of blockchain technology – a voting Web application

Our earlier example about a financial transaction can be modified to be used for voting. Instead of money we can use a single vote as a digital asset transaction. Validation, safeguarding and preservation of entries are all needed in voting and will be guaranteed by the blockchain technology.

We aimed at designing a decentralized Web voting system, which provides a public and transparent voting process while protecting the anonymity of voter's identity, the privacy of data transmission and verifiability of ballots.

The proposed solution is divided into a Front End layer and a Back End layer. The Front End layer is used by voters during the election phase to log in and cast their votes on a mobile device or a computer. The Back End layer is connected to Ganache, a personal blockchain for Ethereum development, and to the Truffle framework, a Smart Contracts testing network that uses the Ethereum Virtual Machine (EVM). Smart Contracts are used together with blockchain technology to trigger actions when some preprogrammed conditions are triggered and are automatically enforced by computer protocols. To code the trigger events, we use Solidity, an object-oriented programming language for writing Smart Contracts. Solidity was designed to work with blockchain platforms like Ganache or Ethereum. As a gateway to our blockchain application, we use MetaMask tool. As the development environment, we use Visual Studio along with Node.js as a JavaScript runtime.

The front end was developed for a fictitious national election in Nigeria with two candidates.

Since it is a proof of concept, we decided to show the tally of votes in the application itself for ease of testing.

During the election, those who are legible to vote log on to the website to register with their designated cryptographic addresses (see Fig. 2).

Then, through utilizing MetaMask, the application performs a verification process of those who are participating in the voting to verify that they're indeed eligible to vote (see Fig. 3).

Next, users participate in the electoral process by choosing a candidate (see Fig. 4). This process is guided by Smart Contracts tool.

The result of the voting is recorded and locked until voting is concluded. After the election is over, the number of votes is counted and presented (see Fig. 5).

4. Discussion

The proposed Web application for elections is based on blockchain technology and Smart Contracts and provides an easily accessible voting system while also verifying the voters eligibility to cast their votes and securely protecting the casted votes. The use of underlying technology can offer multiple benefits in the electoral sphere, some of which are:

- The casted votes would be safely and securely stored in the blockchain ledger. This eliminates any form of manipulation or tampering, for example, the deletion of legitimate votes or the addition of illegitimate votes.
- The casting of votes and tallying of the votes would be a lot quicker while also providing better transparency and accuracy.
- Not many polling stations need to be set up since the voters can vote on their computers or mobile devices. This helps to reduce the cost associated with setting up and running polling stations.

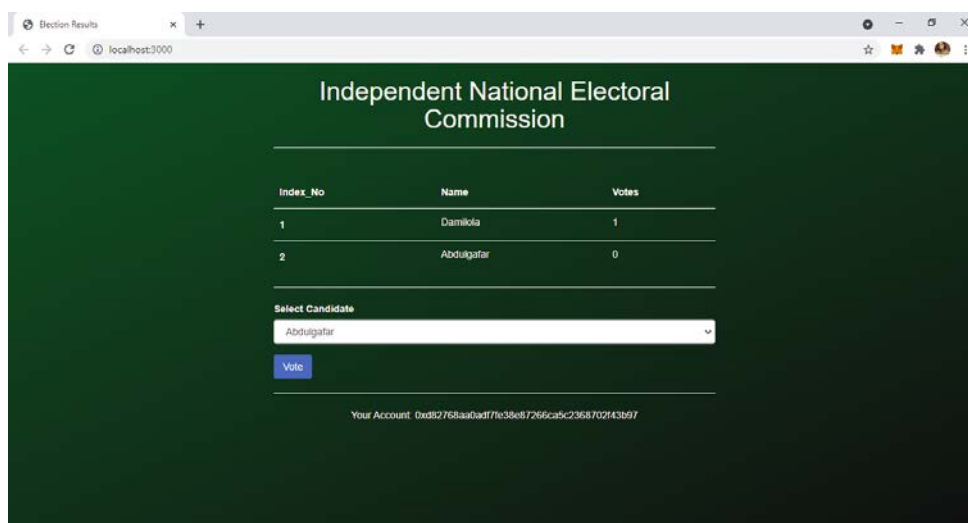


Fig. 2. Voting web application screen

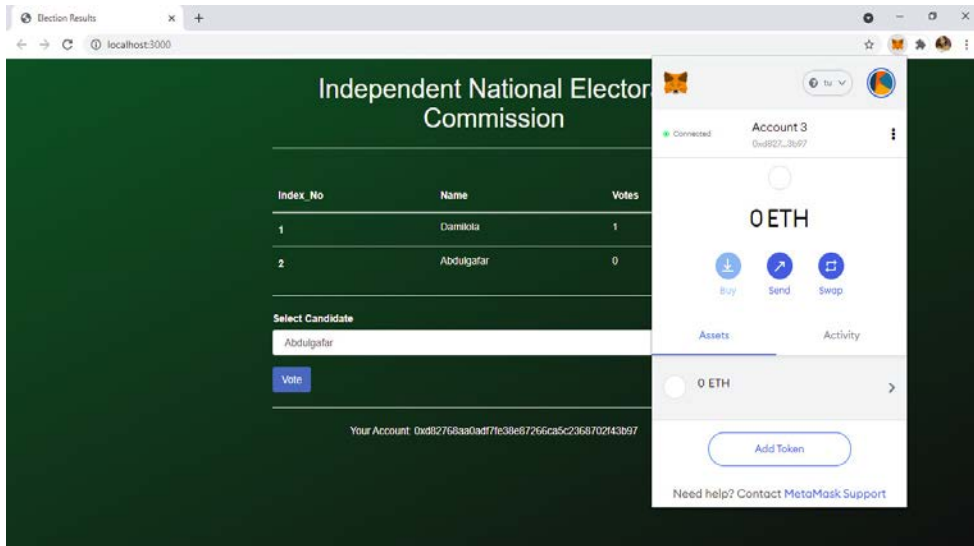


Fig. 3. User MetaMask verification

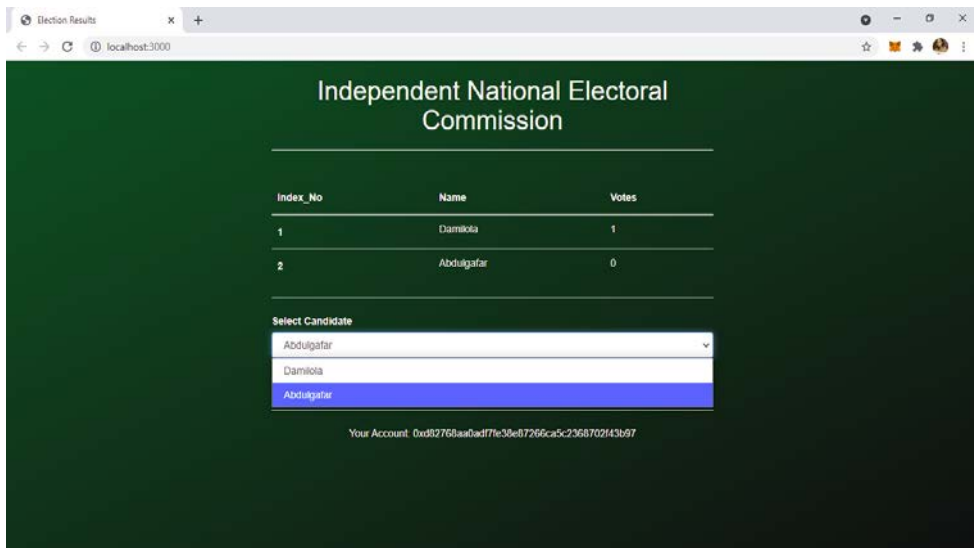


Fig. 4. Voting choice



Fig. 5. The results of voting

– Voters are not required to leave their homes or place of work to cast their votes. This eliminates the need for declaring a public holiday on the day of elections.

– More younger people might participate in elections as the result of utilizing technology accessible through smart phones and computers.

There are certainly some major disadvantages of such an approach, among which are:

– Access to a computing device is required.

– Technological maturity is necessary.

These problems might and will exclude some population from voting. A natural solution is to use a mixed approach wherein paper ballots are provided as a backup on a few polling stations.

All in all, blockchain technology is appropriate for using as an election mechanism, which was showcased as a proof of concept in this paper.

REFERENCES

1. Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE International Congress on Big Data, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.
2. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* Vol. 21, Issue 2, pp. 1676–1717.
3. Biryukov, A., Khovratovich, D. & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 15–29.
4. Pawlak, M., Guziur, J. & Poniszewska-Marańda A. (2019). Voting Process with Blockchain Technology: Auditable Blockchain Voting System. *Advances in Intelligent Networking and Collaborative Systems. INCoS 2018. Lecture Notes on Data Engineering and Communications Technologies*, Vol. 23. Springer. doi: 10.1007/978-3-319-98557-2_21.
5. Khan, K. M., Arshad, J. & Khan, M. M. (2018). Secure Digital Voting System Based on Blockchain Technology. *International Journal of Electronic Government Research (IJEGR)* Vol. 14, Issue 1. doi: 0.4018/IJEGR.2018010103.
6. Hsiao, J. H., Tso, R., Chen, C. M. & Wu, M. E. (2018). Decentralized E-Voting Systems Based on the Blockchain Technology. *Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering*, Vol. 474. Springer. doi: 10.1007/978-981-10-7605-3_50.
7. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M. & Hjálmtýsson, G. (2018). Blockchain-Based E-Voting System. *IEEE 11th International Conference on Cloud Computing (CLOUD 2018)*, pp. 983–986. doi: 10.1109/CLOUD.2018.00151.
8. Huang, J., Debiao, H., Obaidat, M. S., Vijayakumar, P., Luo, M. & Choo, K.-K. R. (2021). The Application of the Blockchain Technology in Voting Systems. *ACM Computing Surveys*, Vol. 54, Issue 3, pp. 1–28. doi: 10.1145/3439725.
9. Çabuk, U., Adiguzel, 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.* Vol. 7, Issue 03, pp. 124–134. doi: 10.17148/IJARCCE.2018.7324.
10. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *Int. J. Netw. Secur. Appl.* Vol. 9, Issue 3.