Blockchain-based biometric election system

Ketevan Tsomaia, Archil Prangishvili, Levan Imnaishvili, Maguli Bedineishvili

Abstract **-** The use of biometric technology in the electoral process has undoubtedly produced positive results in terms of protecting the electoral process, speeding up the results and enhancing the feeling of objectivity among the voters. But there is still room for falsification of election results, as the number of votes received by the candidates and the used ballot papers are kept centrally. It is also important to ensure the reliability of the templates for the biometric characteristics of the voters. In order to solve these problems, this work proposes the distributed database of key data, in particular, the blockchain storage technology. The electoral process scheme and the blockchain-based biometric election system architecture and protocols are elaborated according to the proposed method.

Keywords **-** Biometrics, blockchain, electronic voting system.

I. Introduction

With the development of high technologies, the interest and motivation for applying them in the electoral process has increased dramatically. First of all, this is due to the fact that, despite repeated attempts [1]-[3], the method and system for conducting the electoral process electronically and reliably (without falsification) has so far failed. Biometric technologies effectively solve the problem of voter identification and eliminate the problems of falsification associated with both voters' lists and voting. With the refinement and availability of biometric systems, the interest in applying them in the electoral process has increased [4]-[5]. However, much more could be done for the improvement of election systems. Apart from voter identification problem, huge importance should also be paid to securely maintaining voters' biometric indicators, filled bulletins and election results. Blockchain seems to be a good solution for solving these issues, as it has decentralized database structure, where changing information is not possible without a notice. That is why various election systems based on blockchain technology are designed or being in development process [6]-[10].

With this work[1], we propose the new architecture of election system, where blockchain technology, together with biometrics is used. Blockchain ensures secure data saving and voting while biometrics solve user identification problem.

II. The Problems with the Use of Biometrics in Election System

The use of biometric technologies in electoral systems is very promising at first glance as it solves the problem of high voter identification. However, it still has problems with the identification reliability.

According to the Technical Document about FAR, FRR and EER there are three types of typical errors in biometric technologies [11]. To minimize these errors, the authors of Biometric Electoral System [12] suggest to use b_k $(k = \overline{1,l})$, one of several different biometrics during the voting process. First of all, the selection and use of the relevant from several biometric indicators during the voting process is difficult and uncomfortable for the voter. This problem is solved by a method of prioritization of biometric indicator, which involves evaluating the quality of the biometric indicator at the time of voter registration and using a better-quality biometric indicator during the electoral process. This simplifies the use of the required biometric indicator in the voting process. It should also be noted that the person's biometric indicator is not changed with time, but the quality is improved. It should be borne in mind that there may be a great time difference (several years)

[1]This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSF).
Grant number: PhDF-18-494.
Ketevan Tsomaia is PhD Student at Georgian Technical University, at Computer Engineering Department. Tbilisi, Georgia. keta.comaia@gmail.com
Archil Prangishvili is Professor at Computer Engineering Department at Georgian Technical University. Tbilisi, Georgia. a_prangi@gtu.ge
Professor Levan Imnaishvili is Head of Computer Engineering Department at Georgian Technical University, Tbilisi, Georgia. L.imnaishvili@gtu.ge
Maguli Bedineishvili is Associate Professor at Computer Engineering Department at Georgian Technical University, Tbilisi, Georgia. M.bedineishvili@gtu.ge

between the registration process of the person and the voting process. The biometric electoral system is an electronic technology and can therefore become the target of cyberattacks. First of all, this is due to data processing and centralized storage. Cyberattacks also make it difficult to keep centralized biometric templates of voters b_k $(k = \overline{1,l})$. In case of losing the biometric templates of voters, their restoration or replacement, unlike the authentication password, will not be possible [13], and therefore biometric elections are not reliable in data security.

III. The Prospects for using block chain in election systems.

Block chain is a distributed database of interconnected data blocks by cryptographic methods [14], making it the most secure database.

Election system block chain architecturally is an integration of all the computers subordinated to the central electoral body into a single network. Thus, the computer technology of the biometric election system should be used to organize the block chain network. The authors of Information and Computer Technology, Modeling and Control [12], presented the architecture of the electoral system, which includes registration and voting terminals at polling stations, being the combination of personal and console computers.

Also, the computer technology of other organizations or NGOs may be included in a single network.

Blockchain is characterized by a data storage procedure that is characterized by a large amount of data storage time.First, data storage time depends on the amount of data and the number of nodes involved in the blockchain.Therefore, for such a large-scale event as the conduct of an electoral process nationwide, it is necessary to store in the blockchain the necessary data sensitive to the electoral process fraud. In the biometric election system, the following data are:

- Number of votes accumulated by the candidates.
- Voters biometric indicators templates.
- Ballot papers used by voters and thrown into the ballot box.

Therefore, the following structure of the blockchain data repository is revealed:

- p_i $(i = \overline{1,n})$ private storage voter (PSV).
- t_k^i $\left(k = \overline{1,l},\ i = \overline{1,n}\right)$ biometric reference template storage (BRTS).
- c_j $(j = \overline{1,m})$ repository of the candidate to be elected.
- b_i $(i = \overline{1,n})$ repository of the ballots (including void and canceled ballot papers).

All storages have the corresponding public and private key. A pair of n keys to the PSV is generated when registering a subject as a voter of s_i $(i = \overline{1,n})$.

The PSV closed key is owned by the voter in the form of a QR code card (the card also contains the p_i $(i = \overline{1,n})$ voter's personal number, first name, last name) and the open key is owned by the central election authority. All other repository key pairs are generated during the run of the system and are owned by the CEC. p_i voter PSV, in turn, includes:

- Personal number.
- Biometric templates t_k^i $(k = \overline{1,l})$.
- Identification codes for biometric templates.
- Election participation status (current vote status: 0 or 1).
- Filled ballot paper (either canceled or annulled).

Unified repository of biometric indicators of voters includes:

- t_k^i $(k = \overline{1,l},\ i = \overline{1,n})$ biometric templates.
- N identification codes for biometric templates.

The repository of candidate votes includes:

- c_j candidate's personal number, name, surname.
- c_j count of votes received by the candidate.

IV. The blockchain-based biometric election system architecture and protocols

The biometric electoral process involves two stages: compiling biometric voter lists and biometric voting directly in the electoral process.

Therefore, two systems are needed to conduct the electoral process: the voter registration system and the voting system.

A. The Architecture of the Voter Registration System

The system is a combination of the subject-voter registration terminals and the central electoral body server [12], integrated into a computer network. The registration terminal is a personal computer with a biometric sensor, QR code scanner and printer attached to it.There is no need to use QR code scanner to register subject as a voter, but it is used to update templates t_k^i $(k = \overline{1,l})$ of biometric indices of an already registered p_i subject.

The CEC server is linked to the blockchain. The database of the Central Election Commission server contains the voter list with identification data:

- Personal number.
- Name and surname.
- Date of birth.
- Election number of the subject.

- Registration polling station identifier.

The system provides $t_k^i\ (k = \overline{1,l})$ layout and placement of the biometric indices of the p_i subject in the blockchain.

B. Subject voter registration protocol and algorithm

At the moment of starting the registration process as a voter of a particular p_i:

- The server database contains voter lists and their identification data.
- The blockchain BRTS contains biometric templates for registered voters $p_i\ (i = \overline{1,q},\ q<n)$ $t_k^i\ (k = \overline{1,l},\ \mathrm{i} = \overline{1,\mathrm{q}})$ Identification codes for biometric templates. Obviously, if i = 1, then $t_k^i = 0$. Subject-voter registration protocol and algorithm:
- Prior to enactment of registration terminals, $p_i\ (i = \overline{1,q})$ of biometric templates $t_k^i\ (k = \overline{1,l},\ \mathrm{i} = \overline{1,\mathrm{q}})$ of voters already registered from the Blockchain BRTS and relevant identification codes shall be downloaded in the server. The server uses the corresponding closed key for this purpose.
- In the registration terminal, the operator enters the personal number of the subject p_i, which will be sent to the server, where it will be verified in the electoral list.
- If there is a subject p_i in the electoral list, consent for subject registration will be sent from the server to the registration terminal.
- On the registration terminal, the samples of the subject's biometric indices are formatted and transmitted to the server.
- The server compares the newly formed biometric patterns with the biometric templates of the already registered voters $t_k^i\ (k = \overline{1,l},\ \mathrm{i} = \overline{1,\mathrm{q}})$ [15].
- In case of a positive decision to register to the server, a pair of PSV open and closed keys is formed in the subject block p_i, the closed key is sent to the registration terminal.
- Registration at the terminal is done by printing the closed key of the subject p_i.
- Server blockchain BRTS will include biometric templates for p_i subject $t_k^i\ (k = \overline{1,l})$ and the corresponding identification code.
- The personal number of the subject, the identification code, biometric templates $t_k^i\ (k = \overline{1,l})$ will be recorded in PSV using p_i subject closed key.
- The process continues for other voters.

C. The protocol and algorithm updating voter biometric indicators

- In the registration terminal p_i the closed key of the voter is scanned and sent to the server.
- The server downloads biometric templates of voters already registered from the Blockchain BRTS and relevant identification codes to the server.The server uses the corresponding closed key for this purpose.
- The server uses the p_i closed voter key and downloads the biometric template identifier from the blockchain personal PSV.
- From the biometric templates of registered voters p_i biometric templates according to the voter ID code $t_k^i\ (k = \overline{1,l},\ \mathrm{i} = \overline{1,\mathrm{q}})$ the biometric patterns of this voter $t_k^i\ (k = \overline{1,l},\ )$ is removed.
- At the registration terminal p_i biometric samples of the voter are formed and sent to the server.
- The server compares the newly formed biometric patterns to the biometric templates of already registered voters applying the $t_k^i\ (k = \overline{1,l},\ \mathrm{i} = \overline{1,\mathrm{q}})$ identification method.
- If a positive decision is made to upgrade to the server, the templates $t_k^i\ (k = \overline{1,l})$ will be inserted into the PSV of the voter using the subject closed key p_i. The same templates will also be added to the BRTS.

D. Architecture and function of the blockchain-based election process management system

The system provides for the voters voting at polling stations and remotely.

The polling station includes:

- Registration terminals.
- Voting terminals.
- Local polling station server.

All terminals and local servers are united in the local area network.Local server is also connected to the central election commission server on a computer network. All the terminals and local servers at the polling station are on the blockchain.

The registration terminal is equipped with biometric sensors and a QR code scanner, the voting terminal is equipped with biometric sensors.

The remote voting terminal is a personal computer equipped with biometric sensors and a QR code scanner.The remote voting terminal on a global network is connected to the central election commission server.

Prior to the start of the electoral process, the voters' list with the identification data is posted on the Central Election Commission server. At the moment the blockchain contains $p_i\ in\ the\ voter\ PSV$:

- Personal number.
- Biometric templates$t_k^i\ (k = \overline{1,l})$.
- Identification code for biometric templates.
- Election participation status is 1.
- Filled ballot paper repository is empty.

The ballot box contains:

- Name and surname of the candidate.
- Counted votes are empty.

The repository of used bulletins is currently empty. Before the start of the election process:

- Candidates' personal numbers, names and surnames are downloaded from the repository of candidates for blockchain on the CEC server.
- N ballot paper is generated at random in the CEC server.
- Voting lists by precincts will be uploaded to local subsystem servers.
- The closed key of the ballot paper repository will be sent to the polling stations.

Upon completion of the election process, the system uses the lock keys of the candidates for blockchain and downloads the values of the candidates' counters to the server.

E. Voting from the polling station

There are two phases of voting at the polling station:

- Voter registration.
- Voting directly.

Voting algorithm

- For registration, the p_i voter represents the QR code of the private locked key.
- The QR code of the closed key is scanned at the registration terminal.
- The registration terminal adjusts the p_i closed key of the voter to the open key of all voters.
- If set to one of the open keys, the blockchain PSV from the local server will receive the biometric patterns of the voter $t_k^i\ (k = \overline{1,l})$ and the value of the voting status equal to one at the moment.
- Voter registration permission is issued from the local server at the registration terminal.
- The registration terminal prioritizes one of the biometric parameters of the voter and forms the corresponding k biometric sample, which is then transmitted to the local server.
- In the local server, from $t_k^i\ (k = \overline{1,l})$ is separated k and compared to the biometric sample of the voter.
- If a positive decision is made to register with a local server, the electronic bulletin will be received from the CEC server.
- The e-bulletin will be sent to the voting terminal.
- If a voter has filled out an e-bulletin, the filled-in bulletin will be recorded into the blockchain repository and PSV. Also the value of the voting status in PSV will be -0. At the same time, the CEC server uses the closed key repository of the candidate to vote and, consequently, the candidate's vote count is increased by one unit.
- If the voter has not entered the voting booth or has not used an electronic ballot paper, then the polling station administrator cancels the unused ballot paper from the local server. Accordingly, the annulled bulletin will be copied to the blockchain repository and PSV. Also the value of voting status in PSV will be zero.

F. Voting remotely

The voters go to the Voting Website and carry out the following procedures:

- p_i voter scans QR code of the private locked key.
- The CEC server adjusts the p_i closed key of the voter to the open key of all voters.
- If set to one of the open keys, the blockchain PSV from the server will receive p_i voter biometric templates $t_k^i\ (k = \overline{1,l})$ and the voting status value is one at the moment.
- An electronic ballot paper will be displayed on the voter's personal computer monitor.
- p_i voter l uses biometric indices to prioritize one and therefore k biometric patterns are transmitted to the server.
- The server separates k template from $t_k^i\ (k = \overline{1,l})$ and compares the biometric pattern of the voter with it.
- In case of making a positive decision in the server, it is considered that the voter has filled out the e-bulletin. Filled ballots will be copied to Blockchain's used ballot repository and PSV. Also the value of voting status in PSV will be zero. At the same time, the server uses the closed key repository of the candidate to be selected and, consequently, the candidate's vote count is increased by one unit.

G. Verification of the votes by the voters

To verify the vote, it is enough to equip the PC with a QR code scan.

The voter carries out the following procedures:

- p_i voter scans the QR code of the private locked key.
- The CEC server adjusts the p_i closed key of the voter to the open key of all voters.
- In case of adjusting to one of the open keys, the blockchain PSV will receive the bulletin used by p_i voter from the server, supplied to the voter's personal computer.

V. Assessment of the Reliability of the Blockchain-Based Biometric Election System

Business process analysis of conducting electoral elections shows that the electoral process includes four

main components: voter identification, data transmission, data processing and data storage. Accordingly, there is a probability of securely (without falsification) managing these constituents: $P_i^{id} - i\ (i = \overline{1,n})$ for voter identification, P_i^{dt} for data transmission, P_i^{dp} for data processing and P_i^{ds} for data storage. The reliability of data transmission depends on the number of transmission channels, software and hardware and the amount of transmitted data. The security of data processing is based on the number of processor nodes, software and hardware and the amount of data. Data storage reliability depends on the method of data storage, the number of repositories, software access to data and the amount of data. For these last three components let's assume that m is the number of components.

Therefore, the reliability of each component stand for the system will be: $R_{sys}^{id} = \prod_1^n P_i^{id}$, $R_{sys}^{dt} = \prod_1^m P_i^{dt}$, $R_{sys}^{dp} = \prod_1^m P_i^{dp}$ and $R_{sys}^{ds} = \prod_1^m P_i^{ds}$. Consequently, overall reliability of the electoral election system will be: $R_{sys} = R_{sys}^{id} * R_{sys}^{dt} * R_{sys}^{dp} * R_{sys}^{ds}$. In case of blockchain based biometric election system, with the high probability we can assume that $R_{sys}^{id} = 1$ and $R_{sys}^{ds} = 1$. Thus, for such a system $R_{sys}^{*} = R_{sys}^{dt} * R_{sys}^{dp}$. Accordingly, $R_{sys}^{*} < R_{sys}$.

VI. CONCLUSION

The use of biometric technology in the electoral process has some benefits in terms of protecting the electoral process from fraud, speeding up the results and raising the feeling of objectivity of the voters. At the same time, electronic election systems are the target of cyberattacks as they use centralized databases. The problem can be solved by incorporating blockchain into the biometric election system architecture. The method of storing sensitive data to falsification of the biometric election system, such as templates of biometric indicators of voters, used ballot paper storage in the block chain is proposed. Accordingly, the blockchain-based biometric election system architecture, the process control and management protocols are developed.

REFERENCES

[1] Schneier, B. What's Wrong with Electronic Voting Machines? https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html

[2] Debrah, E., Effah, J., Owusu-Mensah, I. Does the use of a biometric system guarantee an acceptable election's outcome? Evidence from Ghana's 2012 election. African StudiesVolume 78, Issue 3, 3 July 2019, Pages 347-369.

[3] Narayanan, N.P., Pradeep, C.S., Gulati, P., Bharath, G.R.,Nivash, S. Design of highly secured biometric voting system. International Journal of Engineering and Advanced Technology,Volume 8, Issue 5 Special Issue 3, July 2019, Pages 111-114.

[4] Mohammed Khasawneh ; Mohammad Malkawi ; Omar Al-Jarrah ; Laith Barakat ; Thaier S. Hayajneh ; Munzer S. Ebaid. A biometric-secure e-voting system for election processes. IEEE, 2008 5th International Symposium on Mechatronics and its Applications. October 2008, INSPEC Accession Number: 10299059. DOI: 10.1109/ISMA.2208.4648818

[5] Kiran S. Dhawale1, Darshika R. Ingole, G. A. Dashmukhe. Online Voting System Based on Fingerprint and Aadhar ID. International Journal of Research in Engineering, science and Management. Volume-2, Issue-2, February-2019. www.ijresm.com ISSN (online): 2581-5792.

[6] Montes D. Juan, Rincón P. Andrés, Páez M. Rafael, Ramríez E. Gustavo, and Pérez C. Manuel. A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain. International Journal of Modeling and Optimization, Vol. 8, No. 3, June 2018, Pages 160-165.

[7] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, Ningxiao Lu. Large-scale Election Based On Blockchain. 2017 International Conference on Identification, Information and Knowledge in the Internet of Things. Procedia Computer Science 129 (2018) 234-237.

[8] Snehal Kadam, Khushaboo Chavan, Ishita Kulkarni, Prof. Amrut Patil. Survey on Digital E-Voting System by using Blockchain Technology. International Journal of Advanced Scientific Research and Engineering Trends. Vol. 4. Issue 2, February 2019, ISSN (online) 2456-0774. Pages 5-8.

[9] Prof. Hiren M Patel, Prof.Milin M Patel, Prof.Tejas Bhatt. Election Voting Using Block Chain Technology. International Journal of Scientific Research and Review. Vol. 07, Issues 05, May 2019. ISSN No.:2279-543X. UGC Journal No.: 64650.

[10] Noor Mohammedali, Ali Al-Sherbaz. Election System Based on Blockchain Technology. International Journal of Computer Science & Information Technology (IJCSIT) Vol 11, No 5, October 2019. Pages 13-31.

[11] Technical Document about FAR, FRR and EER. by SYRIS Technology Corp., 2004.

[12] Information and Computer Technology, Modeling and Control. Chapter 4. A.Prangishvili, L. Imnaishvili, M. Bedineishvili and N. Kirkitadze, Biometric Electoral System. Novapublishers, 2017.

[13] Patel, V.M., Ratha, N.K., Chellappa, R. Cancelable biometrics: A review. (2015) *IEEE Signal Processing Magazine*, 32 (5), art. no. 7192838, pp. 54-65.

[14] Zibin Zheng, Shaoan Xie1, Hongning Dai, Xiangping Chen, Huaimin Wang . An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends. 6th IEEE International Congress on Big Data, June 2017, pp. 557-564.

[15] Anil K. Jain,Arun Ross, Salil Prabhakar. An Introduction to Biometric Recognition. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.