- 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.