

PAPER • OPEN ACCESS

Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root

To cite this article: S. Aruna *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **993** 012103

View the [article online](#) for updates and enhancements.

You may also like

- [A Cost-Efficient Proof-of-Stake-Voting Based Auditable Blockchain e-Voting System](#)
Trishie Sharma, C Rama Krishna and Arshdeep Bahga
- [E-Voting System Using Homomorphic Encryption Technique](#)
A.C. Santha Sheela and Ramya. G. Franklin
- [A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication](#)
T. P. Abayomi-Zannu, I. A. Odun-Ayo and T. F. Barka



The Electrochemical Society
Advancing solid state & electrochemical science & technology

241st ECS Meeting

Vancouver, BC, Canada. May 29 – June 2, 2022



ECS Plenary Lecture featuring
Prof. Jeff Dahn,
Dalhousie University



Register now!



Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root

S. Aruna¹, M. Maheswari² and A. Saranya³

¹Assistant Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India.

²Associate Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India.

³Assistant Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India.

E-mail: arunas@srmist.edu.in, maheswam@srmist.edu.in, saranyaa2@srmist.edu.in

Abstract. Over the course of time, electronic voting has evolved as a substitute for paper ballot voting to decrease redundancies and inconsistencies. Due to the many security and privacy vulnerabilities experienced over time, the past results of e-voting in the last three decades indicate that it has not been very successful. All cryptocurrencies are actually based on block chain. Block chain is based on the principle of distribution and decentralization. It is a continuous and continuously growing ledger that holds, in a secure, chronological and immutable way, a permanent record of all the transactions that have taken place. Value in a block chain can be anything. In the case of cryptocurrencies, it takes the meaning of money or currency. While in a game it takes the form of points or score. The value can take the form of a vote or a ballot while e-voting. The blockchain can be used in this article to pass votes between two parties. In our case, the electorate is one party and the candidate who earns the vote is the other. Without having a controlling central authority body, the block chain can be implemented in a more stable manner in mass electoral voting practise. A voting system that uses a more stable, tamper-proof block chain (immutable to voting modifications either by other voters or by any third party) and is cost-effective.

Keywords- Block chain, Electronic Voting, Cryptocurrency, Decentralization, Distributed ledger

Introduction:

E-VOTING is amidst the popular public segments that have the scope to be improved by Blockchain technology. The idea here is simple. Blockchains can address two of the most prevailing problems common in voting today which are the voter's access and voter's fraud. Blockchain enabled e-voting will deploy an encrypted key (such as an RSA private key) and tamper-proof personal IDs (Fingerprint biometric verification). Blockchain will tie each cast/vote of the ballot to an individual voter to establish a permanent, immutable record so that no hacker will be able to engage in reprehensible pursuits because such no operation can be performed on all of the public ledgers such as blockchain that are a part of a peer-to-peer consensus network and also to do that one would need to recalculate all the hashes of every block from the infected block which will be very time consuming and too complex to perform. To exploit the used network or any blockchain network, the hackers would have to hack all of the blocks (blocks containing even one transaction record) even before the new ones got introduced. The hashes of hashes will be there to ensure that no vote has been altered or removed and also that there are no illegitimate votes casted or the original vote changed. In simple words, blockchains enables the formation of tamper-proof audit trails or traces of voting. In the presented report, we would try to highlight some blockchain-enabled e-voting methodology and



its results and conclusion. The e-voting is foreseen to have an incredible future yet the past isn't excessively sublime. There are some countries that are trying to bring up e-voting but the problem of reliability and proof which are among the other stuff that need immensely deep consideration by the governments and technological people and basically the people. This research suggested a system based on the adaptable block chain that could capture the issues that prevail in the polling process, and would help in the selection of a suitable hashing algorithm, is helpful even in the selection of changes in the blockchain, it will help in securing the content of block data. Block-chain has been of great use in order to fit into the available needs and process of electronic voting.

Related Works:

Nir Kshetri [3] each voter is considered as a wallet, and the transactions between wallet is limited to one. As the candidates are considered as the receiver wallet. The vote is actually the transaction between all the candidates or receiver wallets. The methodology used in this paper is Blockchain enabled e-voting which is using an encrypted key along with the alteration-proof user IDs. The advantage is Blockchain enabled e-voting will help us to ensure the aspect of security as well as transparency which would help to reduce electoral violence and produce more mathematically precise voting results. The Disadvantage is They did not use a decentralized voting system (only meant for one single place). No consensus. The wallet-coin model can be amended to single wallet.

Fridrik [2] Attempt to use a case study to determine the potential of distributed ledger technologies; such as the election process and its implementation via a block-chain-based framework, which will boost security and reduce the cost of conducting national elections. The technique is to achieve these objectives by using a Go-Ethereum Proof-of-Authority (POA) blockchain authorization setup. They have used the algorithm through a process based on identity as a stake, which delivers faster transactions. They use district and boot. The voting data is checked by the majority of the district nodes when any individual elector casts a vote from their compliant smart contract, and any vote they agree on is appended to the blockchain. The advantage is Elections can be used as a Blockchain part of Smart Contract, using developer friendly Framework (Go-Ethereum), Centralized consensus. The disadvantage is limited up to 5000 votes/second. Can use some better blockchain frameworks for increasing transactions per second.

Zhang [4] proposes a local voting mechanism conceptualized on block-chain to help decision making for its peers' networks. It protects the privacy and enables detection as well as correction against cheating. The methodology used are Distributed consensus based blockchain algorithm. The advantage is Elections can be used as a Blockchain part of Smart Contract, Peer to peer network, consensus, Two phase validation (decryption pvt key, smart contract verification). The disadvantage is No proof if the model will work or not. Untested with many blockchain frameworks. Can use a better blockchain framework for increasing transactions per second. If tested with faster and premised blockchain frameworks it can set the standards.

Crowcroft[1], to ensure data protection, such as block formation and sealing, it proposes useful hashing techniques. The methodology used are consensus based blockchain algorithm. The advantages are Used their own framework, Better hashing algorithm. The disadvantage is No proof if the model will work or not, Untested with many blockchain frameworks.

Proposed Architecture:

E-voting has developed over time to be an auxiliary to the paper-based voting to reduce mistakes as well as complete vote counting process faster. But flaws of safety, secrecy have been there, as it comes it every electronic technology. This is a grave liability, as electronic voting is used in election of governments of countries. Block is the primary component of any block-chain which contains of a body and a header, In which the body of the block comprises the transactions that are to be written to system and header of block encompasses data about block such as nonce value, time stamp of block and transactions and previous hash. In the block part, the voter casts the vote/ballot after validation that he/she is a valid user. Then ballot signed by using a RSA private key. If the submitted ballot is proven to be valid, it will be sealed. In this chain section, transactions (ballots) with valid data will be generated. They are then sealed into blocks.

Challenges in the Existing Systems are:

Privacy: Only the elector is permitted to see his or her data and who they voted for as well. The revealed details in election is nothing but the cumulative votes to candidates as well as in entire election

Absence of Evidence: While privacy with the concealment component will protect against electoral fraud, there is no way to guarantee that votes are cast under any form of electoral fraud.

Fraud-Resistance: The system should check the uniqueness and status of each probable voter, but should not allow this information to be related to their voting status.

Ease-of-Use: Elections are open to the public, and must therefore be organised in such a way that fewer preparation and technological knowledge can be required.

The project is based on Blockchain which is still a research area, hence a detailed study was required to understand the requirements. Since most of these are only theoretically available in form of research papers, we intend to generate data and then segregate it for detailed study. We have used three methods for requirements gathering analysis are brainstorming, observation and Document Analysis

The main objective of the project is to form a framework for a voting model to ensure the security of the data. Blockchain is secure and can be used for effective casting of votes and ensuring that the voting system is not tampered or manipulated to change the votes. In simple terms the objective of our project is: To verify voters' identity using biometric authentication, face or fingerprint, Make the election process as transparent as possible (independently verify that the process is conducted according to procedures and no irregularities), Tracking of votes for voters (even after the election is over users can check who they voted for), Ability to change their votes any time before the deadline.

In Figure1: System Architecture of Electronic Based Voting System consists of four modules are Voter Registration, Voter Authentication, Vote Process and Blockchain module. In Voter Registration we will ask the volunteering voters to register their fingerprint for biometric authentication. Happens before the actual voting takes place.

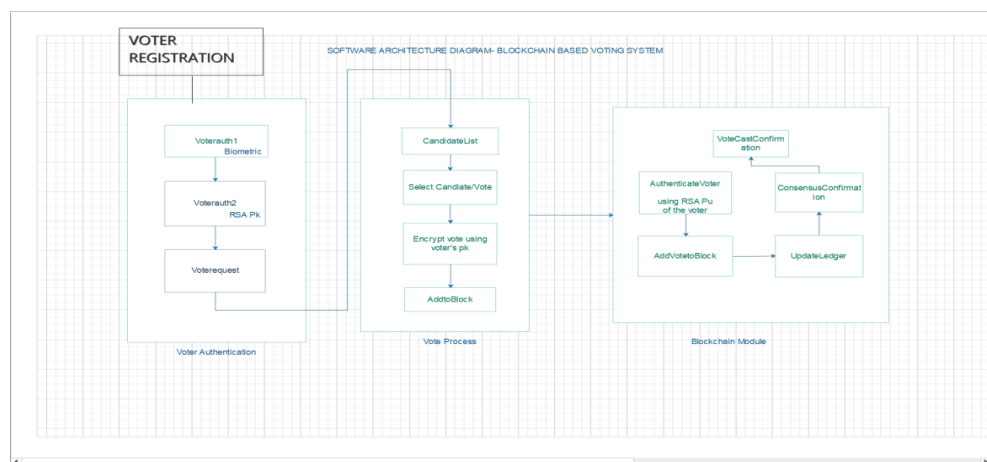


Figure1: System Architecture of Blockchain based Electronic Voting System

In Voter Authentication the voter will be verified by his unique finger impression and the framework will produce a pk for the voter with the goal that vote can be encrypted and decrypted by the blockchain server. In Vote process the candidate list will be generated after successful authentication. The voter will then select a candidate and after selecting vote is encrypted by RSA algorithm and sent to server to add to the blockchain. In Blockchain module the candidate list will be generated after successful authentication. The voter will then select a candidate and after selecting vote is encrypted by RSA algorithm and sent to server to add to the blockchain.

Four Algorithms are used for Securing the database are SHA3, RSA, Blockchain Voting and Merkle root algorithm. In SHA3 Algorithm is used for hashing. A unidirectional feature for producing digital prints of the chosen length (the standard accepts 224, 256, 384 or 512 bits) from input data of any size is also called Keccak. It can directly be implemented by the developer by importing the python module keccak or pysha3[5][8].

Rivest-Shamir-Adleman (RSA) It is one of the most well-known cryptosystems for key transfer and block encryption. In R.S.A we use a block with variable size and a key with variable size. It follows an asymmetric way of encryption. R.S.A has three steps; key generation, encryption and decryption. The voter will then select a candidate to cast vote and after selecting the vote will

then be encrypted by RSA algorithm and sent to server to append in the blockchain. The constituent and vote data that will be passed to the RSA input and the data will be used as type string, then it will be encrypted using RSA private key by using RSA algorithm.

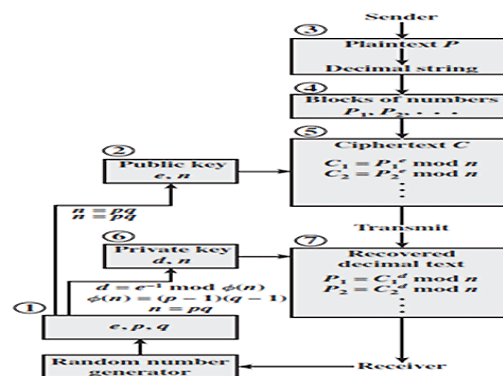


Figure 2: Processing Steps in RSA Algorithm

In Blockchain[7] voting Algorithm every vote we will be asked to seal the ballot which will generate a ballot id and a generated signature. After sealing the ballot, the transaction hash will be generated and stored then the block hash will be created with the updated hashes and a unique nonce will be given to each block with a time stamp. Figure 3 gives the block details of voting system after hashing and Figure 4 gives the verification process of a voter and generated the signature for every ballot.

Block detail

Previous hash	GENESIS
Transaction hash	ede05ff580fbb6e7af5587496f12ad0820891a6bbd335fe2ed8752914f0f8c16
Block hash	0000398a7ddb4a3200d70ac6a494949ea2e1259dc94f1b130850515d911f1d82
Nonce	82395
Timestamp	1583120451.76024 (2020-03-02 09:10:51)
Back to homepage	

Figure3: Single Block details after hashing

Signature Verification

Your ballot was 1dca4d13-faec-40de-04c1-8d8edf6b6d5[1]1502120380.780967

Generated signature
b"b'\x04T\x00'\x02'\x06'\x07'\x0b'\x08'\x09'\x0a'\x0b'\x0c'\x0d'\x0e'\x0f'\x10'\x11'\x12'\x13'\x14'\x15'\x16'\x17'\x18'\x19'\x1a'\x1b'\x1c'\x1d'\x1e'\x1f'\x20'\x21'\x22'\x23'\x24'\x25'\x26'\x27'\x28'\x29'\x2a'\x2b'\x2c'\x2d'\x2e'\x2f'\x30'\x31'\x32'\x33'\x34'\x35'\x36'\x37'\x38'\x39'\x3a'\x3b'\x3c'\x3d'\x3e'\x3f'\x40'\x41'\x42'\x43'\x44'\x45'\x46'\x47'\x48'\x49'\x4a'\x4b'\x4c'\x4d'\x4e'\x4f'\x50'\x51'\x52'\x53'\x54'\x55'\x56'\x57'\x58'\x59'\x5a'\x5b'\x5c'\x5d'\x5e'\x5f'\x60'\x61'\x62'\x63'\x64'\x65'\x66'\x67'\x68'\x69'\x6a'\x6b'\x6c'\x6d'\x6e'\x6f'\x70'\x71'\x72'\x73'\x74'\x75'\x76'\x77'\x78'\x79'\x7a'\x7b'\x7c'\x7d'\x7e'\x7f'\x80'\x81'\x82'\x83'\x84'\x85'\x86'\x87'\x88'\x89'\x8a'\x8b'\x8c'\x8d'\x8e'\x8f'\x90'\x91'\x92'\x93'\x94'\x95'\x96'\x97'\x98'\x99'\x9a'\x9b'\x9c'\x9d'\x9e'\x9f'\xa0'\xa1'\xa2'\xa3'\xa4'\xa5'\xa6'\xa7'\xa8'\xa9'\xaa'\xab'\xac'\xad'\xae'\xaf'\xb0'\xb1'\xb2'\xb3'\xb4'\xb5'\xb6'\xb7'\xb8'\xb9'\xba'\xbb'\xbc'\xbd'\xbe'\xbf'\xc0'\xc1'\xc2'\xc3'\xc4'\xc5'\xc6'\xc7'\xc8'\xc9'\xca'\xcb'\xcc'\xcd'\xce'\xcf'\xd0'\xd1'\xd2'\xd3'\xd4'\xd5'\xd6'\xd7'\xd8'\xd9'\xda'\xdb'\xdc'\xdd'\xde'\xdf'\xe0'\xe1'\xe2'\xe3'\xe4'\xe5'\xe6'\xe7'\xe8'\xe9'\xea'\xeb'\xec'\xed'\xee'\xef'\xf0'\xf1'\xf2'\xf3'\xf4'\xf5'\xf6'\xf7'\xf8'\xf9'\xfa'\xfb'\xfc'\xfd'\xfe'\xff'".hex()

The ballot is signed successfully.

Seal the ballot

Figure 4: Signature Verification of the user

In a **Merkle root** is commonly referred to as the hash of all the hashes of all the transactions that are part of a block in a blockchain. Here the Merkle root is the hash of all the vote transaction inside a block. The number of votes stored in a block depends entirely on our own requirements. To calculate the changing hashes with every new vote added and to create the final hash we will use pymerkle tools algorithm available in python library, can be installed through pip. The module uses SHA-3 algorithm to create the hashes which is faster and more efficient than SHA-1 and SHA-2. A Merkle tree is a data structure tree in which every leaf node i.e. (the node which has no children) stores the hash of the block, and every non-leaf node (the node which has one or more children) stores the hash of its child nodes. So, the root node will contain the hash of all hashes that we need here. In Figure 5 the root node is having the hashes of all the child nodes.

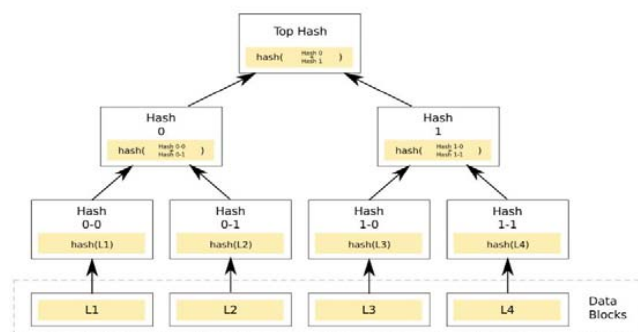


Figure 5: Merkle tree or Hash tree which contains Data Blocks L1, L2, L3, L4 and their hashes and the hashes of their hashes and so on.

The e-voting is foreseen to have an incredible future yet the past isn't excessively sublime. In certain nations e-casting a ballot isn't a choice while few are in a procedure to take out the security, undeniable nature, and anonymity concerns. This examination has proposed a structure dependent on the movable blockchain that can catch the issues in the surveying

procedure, determination of the reasonable hash calculation, choice of modifications in the blockchain, procedure of casting a ballot information the executives, and the security and verification of the democratic procedure. The intensity of blockchain has been utilized customizable to fit into the elements of the electronic voting procedure. We developed an effective model for generating a block for every vote based on blockchain block creation and sealing. The sealed blocks can be used to count the votes for each candidate. For our project we used Python simulation-based test which is a part of Django Framework[6]. It's a python-based unit testing framework based out on Python and helps us easily perform unit testing based on different modules present in the system, thus helping us gain insights on how the software works and how the different modules work independently. We simulated the number of candidates to be 3 and created a simulation class with loosely coupled functions and set the voting time limit to one minute.

When we started the test, we got 10000 votes in one minute (3332+3377+3291) for the three candidates. The votes were successfully sealed in blocks along with the voter id of the voter.

Entity	Test Function	Rate in 1 min
Votes Casted	Vote randomizer function	6756 votes/min
Blocks Created	Block generator function	9 blocks/min
Hashes generated	Block Hash generator	6756 hashes/min

Table 1: Time scores calculated with for block creation and vote transactions per minute.

Figure 6 shows the end result after the completion of voting system and Figure 7 shows the confirmed number of votes scored by every candidate.

List of confirmed votes

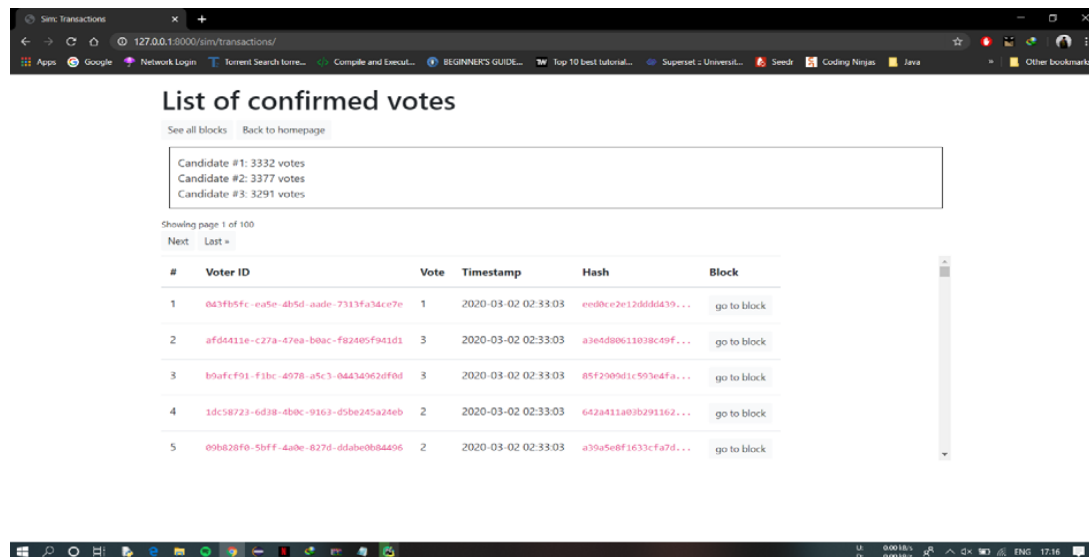
See all blocks Back to homepage

Candidate #1: 55 votes
 Candidate #2: 55 votes
 Candidate #3: 71 votes

Showing page 1 of 2
 Next Last »

#	Voter ID	Vote	Timestamp	Hash	Block
1	043f05fc-ea5e-4b5d-aade-7313fa36ce7e	1	2020-03-02 02:33:03	ee08c2e126550439...	go to block
2	af084118-c27a-47ea-b0ac-f82805f941d1	3	2020-03-02 02:33:03	a3e4880611038c49f...	go to block
3	b9aef01-f1bc-407b-a5c3-0a434062df0d	3	2020-03-02 02:33:03	80f2989d1c593eafa...	go to block
4	1dc50723-6d38-4b0c-9163-d5be2c5a24e0	2	2020-03-02 02:33:03	6428411805b291102...	go to block

Figure 6: Final results after the voting is completed.



List of confirmed votes

See all blocks Back to homepage

Candidate #1: 3332 votes
 Candidate #2: 3377 votes
 Candidate #3: 3291 votes

Showing page 1 of 100
 Next Last »

#	Voter ID	Vote	Timestamp	Hash	Block
1	043fb5fc-ea5e-4b5d-aade-7313fa34ce7e	1	2020-03-02 02:33:03	eed0ce2e12d6dd439...	go to block
2	afd6411e-c27a-47ea-baac-f82405f941d1	3	2020-03-02 02:33:03	a3e4d80611038c49f...	go to block
3	b9afe91-f1bc-4978-a5c3-044349626f0d	3	2020-03-02 02:33:03	85f2909d1c593e4fa...	go to block
4	1dc58723-6d38-4b0c-9163-d5be245a24eb	2	2020-03-02 02:33:03	642a411a03b291362...	go to block
5	09b828f0-5bff-4abe-b27d-ddabe0b04406	2	2020-03-02 02:33:03	a39a5e8f1633cfa7d...	go to block

Figure 7: Confirmed votes of every candidate

Conclusion:

We developed an effective model for generating a block for every vote based on blockchain block creation and sealing. The sealed blocks can be used to count the votes for each candidate. Our proposed System overcome the disadvantage of votes are casted through EVM, There is no way to guarantee that votes are cast in some sort of electoral fraud that only a voter is able to access his / her data and who voted for them. Using SHA3, RSA and Merkel root algorithm all the information about the e-voting system is highly secured in blockchain. Despite the fact that blockchains are exceptionally secure with regards to securing data that is stored in it — the main problem occurs when the clients don't safeguard their private credentials. This implies there is consistently a danger of private keys being taken. As an undertaking or business, you have to teach clients on the best way to protect their private keys.

References:

- [1] Trustworthy Electronic Voting Using Adjusted Blockchain Technology, BASIT SHAHZAD AND JON C ROWCROFT <https://ieeexplore.ieee.org/document/8651451>
- [2] Hjalmarsson, Friarik P., Gunnlaugur K. Hreioarsson, Mohammad Hamdaq, and Gisli Hjalmtysson. "Blockchain-Based E-Voting System." In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986. IEEE, 2018 <https://ieeexplore.ieee.org/document/8457919/figures#figures>
- [3] Blockchain-Enabled E-Voting Nir Kshetri and Jeffrey Voas <https://ieeexplore.ieee.org/document/8405627>
- [4] A Blockchain-Based Network Security Mechanism for Voting Systems Hsin-Te Wu Department of Computer Science and Information Engineering, National Penghu University of Science and Technology <https://ieeexplore.ieee.org/document/8567211/references#references>

- [5] PyCryptodome python based library which contains basic encryption functions <https://pycryptodome.readthedocs.io/en/latest/src/introduction.html>
- [6] Django documentation <https://docs.djangoproject.com/en/3.0/>
- [7] Blockchain technology <https://www.investopedia.com/terms/b/blockchain.asp>
- [8] Python learning <https://docs.python.org/3/tutorial/index.html>