March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

Authenticated Online Voting using Block Chain Technology

S. ThelunguLaxmi[1],Rukesh A P, Suravarapu Rahul Reddy [2]
[1,2]Department Of Information Technology Easwari Engineering College,Chennai, India.
[1]thelungu55@gmail.com, rukeshruk98@gmail.com,[2]rahulrreddy29@gmail.com.

Article Info
Volume 83
Page Number: 8858 - 8865
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 09 April 2020*

Abstract

Voting is a vital duty associated with each and every responsible citizen in a country. This vote plays a major role in deciding the people's leader based on their support among the people. But mostly people neglect their primary duty on behalf of their lethargic character or interest-less [1]. According to a survey in the year 2016 approximately only around 60% of the eligible citizens registered their votes and the remaining 40% percent of the votes were misused for fraud activities like Electoral Frauds and other activities [15]. Thus in order to improvise the number of registered vote, the voting must be made pervasive and available for every citizen around nooks and corners of the country respectively. With the available technologies, any tasks are feasible for implementation. But, every other advancement in technology possesses their equivalent advantages and disadvantages, but for a huge population in the India country the more reliable mechanism available is the block-chain mechanism. The block-chain previously block chain is the collection of continuously increasing list of records or datasets, which supports data-variation without affecting the integrity of the data records in the block chain. The E-voting [14] enables a web-based framework that acquires user's credentials and performs marshalling using the cryptography and associated with the parties optional parameters for the user's selection and the choice obtained from the user is obtained and stored in the database as hash values in the block-chains for security purposes.

Keywords; *The Block-chain mechanism, Marshalling, encrypting, cryptographic algorithms, REST API, Django, Public key Cryptography, Cipher Block Chaining*

I. INTRODUCTION

E-voting [12] is defined as electronic enabled voting that provides security for the user's credentials provided and avoids Electoral Frauds by registering 100% of the vote, since the un-registered voters are imposed with a heavy-duty fine as a punishment. The block chaining [2] is defined as continuously growing list of records called blocks, which are linked and secured with the help of cryptography. Each block is associated with a cryptographic hash value of the previous block and the timestamp that logs the time factor and the transaction date. Built in block-chain is resistive to modification of the data associated with the blocks without affecting integrity of the block-chain. Based on the implementation, e-voting can be electronic voting machines

(EVM) or a computer connected with the internet. In our case, the computer/ any pervasive devices are employed for the implementation enabling ubiquitous computing. The block-chain is typically managed by the peer-to-peer network, where the resources aren't centralized, instead every peer/actor contribute for the resource. In case of peer-to-peer network the network traffic is reduced and congestion is avoided over the network increasing the performance and efficiency. The block-chain are considered to be secure by the design and provided

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

with Byzantine Fault tolerance. A block-chain is decentralized, distributed and public digital ledger that is used to record the public transactions across many computers that cannot be involved with alteration. The main priority of the block-chain mechanism is preserved in the bit-coins transactions, but the voting is related with a huge datasets / records that ought to be public and records every transactions without the ability to alter the data and enabling the user's to perform independently. Each and every block present in the block-chain [3] is associated with a set of information regarding the previous block. It withholds the cryptographic hash value of the previous block. It also comprises of,

Block time- It is the time value that is required to create a separate block associated with the block-chain.

Hard forks- This is the rules/ principles that must be satisfied by the blocks in the block-chain for the periodic updates associated with the block-chain.

Decentralized- By withholding the data/ information amongst the peer-peer network, it reduces the possibilities of the data being attacked or accessed by the malicious sources as of centralized networks.

There are several types of block chains [4] available, they are as follows,

Public block chains –A public block chains has no restrictions for access. Anyone with an internet connection can contribute resources to the block0chain as well as perform validation of the dataset/ blocks present in the block-chain.

Private Block-chains – In this type of block-chain, the block is not added or modified without the permission of the network administrator. The permission are predefined and can only be altered by the administrator. All the other peers are standard actors/users, whereas the network administrator is the master that manages and co-ordinates all the block-chain related tasks.

Consortium Block-chain- This type of block-chain is considered semi-decentralized block-chain since the block are deployed using the distributed network but managed by a single organization more or less as a network.

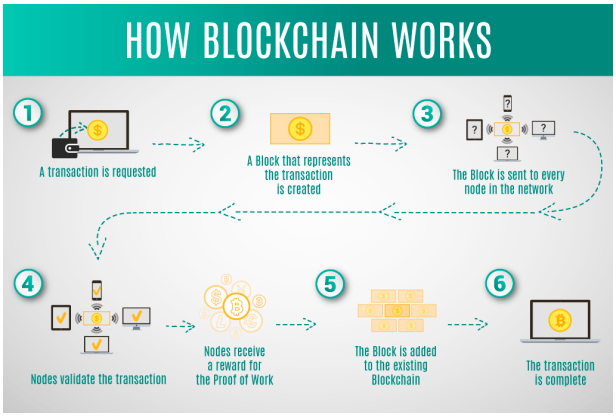

Figure 1.1 Working mechanism of Block Chain

The above Figure 1.1 represents the overall structure of how any transactions associated with the block chaining, they are as follows:

A transaction is initiated

When a transaction is requested for further processing, the block format of the transaction is generated.

The block is transferred to every block available in the block-chain.

The cryptographic functionalities are employed for the process of verification and validation of the block information.

The transaction details are updated and the block is added to the block-chain.

Block-chaining comprises of three major components, they are

Cryptography

Peer-to-Peer Network

Game theory

These components ensure the reliability of the transaction amongst a group of unknown users without a centralized system.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

Sender	The remote host that initiates the transfer using cryptographic hash function
Encipherment	This is the process of converting the message into unintelligible format with the help of the cipher key
Decipherment	This is the process of converting the encoded message into understandable format using the decipher key at the receiver's end/ target host.
Channel	This is the pathway via which the encoded messages are transferred

Table 1.1: Components of Cryptography

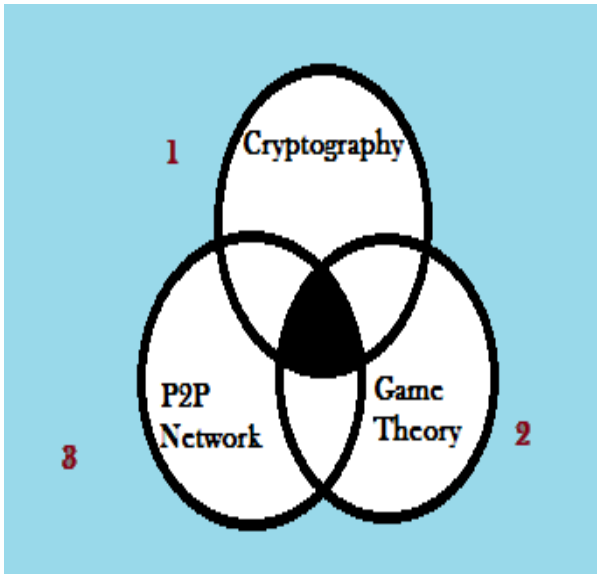

Figure 1.2 Components of Block-Chaining

In the above Figure: 1.2 the cryptography employs three major components [10] are explained in the above table 1.1.Encryption and communication from unauthorized revelation and access of information. The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries. The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender technique can guard the information

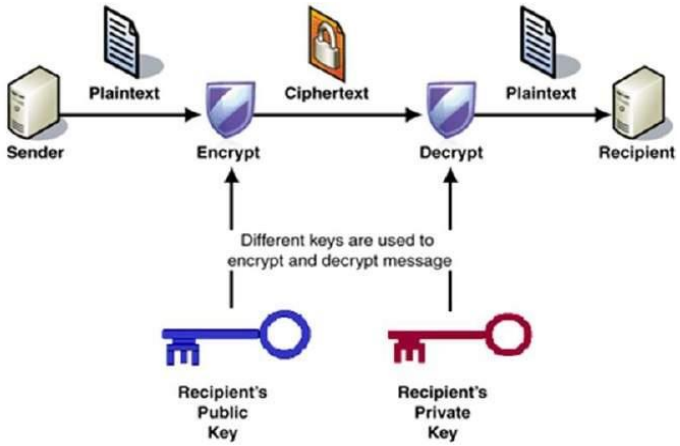

Figure 1.3 Cryptography

In case of the Figure 1.3: block-chain, the transactions are simply locked and unlocked using the signatures, i.e., the Public Key Cryptography [8] is the backbone of the Block-chain network, where the encryption is done using the user's private key that isn't disclosed to others except the user and the decryption is done with the help of user's public key.

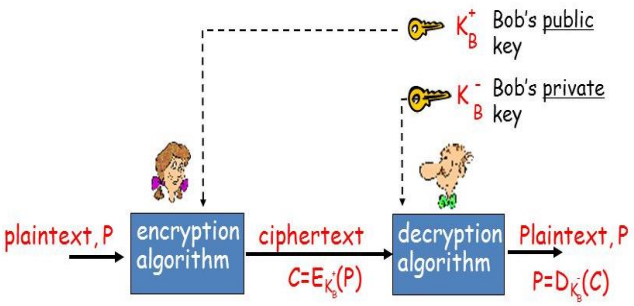

Figure 1.4 Public Key Cryptography

The above Figure: 1.4 depicts the Example where, Alice shares a intimate details with the trustworthy friend Bob by encrypting the message with Bob's public key and transfer the message via the channel to Bob at the other end, who decrypts the message with the private key provided to Bob and extracts the message from the received message.

The Public Key Cryptography is employed in multiple applications with various encryption and decryption algorithms available.

The signature is defined as a unique identification

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

proof associated with the message for sender's identification and authenticity.

Digital signatures are significant element of multiple protocols employed in cryptography. They employ Asymmetric The below Figure: 1.5 represents cryptography that employs two different keys for the marshalling and un-marshalling purposes, they are

Private Key – This is only known to the respective user and not disclosed.

Public key – This key is shared among multiple users for the purpose of encryption and decryption processes.

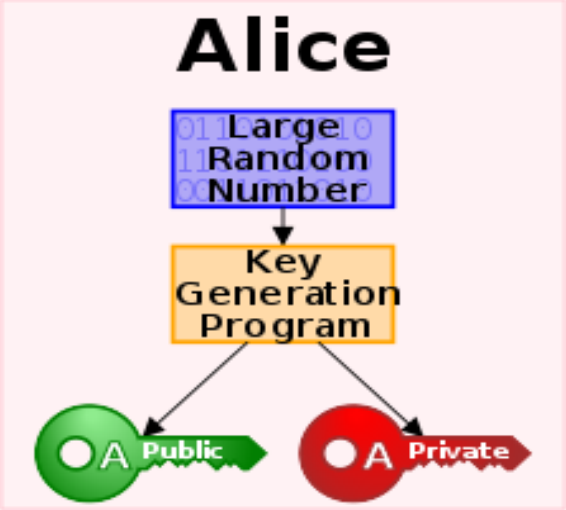

Figure 1.5 Key Generations

II. PROPOSED SYSTEM

The proposed system enhances the methodology of Block-chaining in order to deploy the polling mechanism in much safer and faster manner for the end-users or citizens.

The system comprises of a developed framework using the Python Programming named Django that helps in implementing various data processing and block chaining mechanisms over the web application and easy implementation of the Application Programmable Interface using REST i.e., REST API for the web application, So that the user's polling can be performed ubiquitously without any intervention and attacks. The server side is implemented with Python and PHP which manages the network traffics and congestion over the network thereby improvising the parallel accessing, performance and efficiency.

The advantages of the REST API [23] are as follows:

Stateless client/server protocol: In case normal HTTP Communication, certain variables and headers must be remembered by either client or server, whereas in REST, the stateless transactions are carried using the Cache memory that stores the often accessed variables for faster performance.

Objects in the REST are manipulated from the URL: The REST API obtains the input data via the URL associated with the server accessing and process the input data to provide the output object that is transferred and received via SOAP (Simple Object Access Protocol).

Uniform Interface: The REST also deploys the similar interface as of normal HTTP protocols thereby the interface is uniform and standard.

Layer System: The REST follows a hierarchical layer architecture that enables abstraction of the back-end processes

Use of hypermedia: The hypermedia is the files associated with Multimedia objects such as (Text, Image, Video, and Audio) along the internet that are transferred in the REST API.

The framework emphasizes major parameter for the sake of user login, they are as follows:

The Voter ID number: This is alphanumeric value that is associated with every eligible citizens which is unique for every citizens based on their locality and other details as of for identification.

The Date of Birth of the user: This is a Date-Format that described the DOB of the citizen respectively.

But the above details are employed for easy

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

remembering by the citizens but to enhance the security of the user's privacy details the Cryptography algorithms [6] are employed the HASH Functioning, this function generates a pre-defined length of a hash value i.e., the combination of numerical and alphabets in secure manner using a Hash function. The advantage of hash is that the decoding part, the hash value cannot be decoded as the length of the hash value increases the Brute-Force attack becomes infeasible. Thereby improvising security, the hash value is generated using a key this key is the OTP forwarded to the user's registered mobile number. The OTP is generated in a randomized fashion for each user and is transferred to the registered user's mobile number via SMS Gateway.

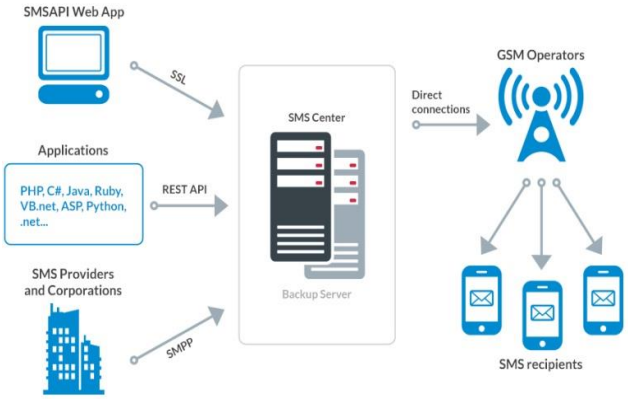

Figure 2.1 SMS Gateway API

The above picture 2.1 depicts the working of SMS Gateway API available that transfers message to the end-users with the help of TextLocal – India's #1 SMS Gateway Platform that provides API for the end-user application integration and abstraction of the backend processes. This gateway provides the interface for Python and PHP also for other platform, which can be integrated with the web-application to deploy messages and perform hashing of the user's privacy details and enabling the interface for polling purposes based on the concern elections being conducted.

AAlgorithm

The algorithm employed in block chaining is described as follows:

Cipher Block Chaining [9]:

Ehrsam, Meyer, Smith and Tuchman invented the Cipher Block Chaining Mode in 1976. In case of CBC each and every block cipher text is Ex-Ored with the successive blocks and the initial block's cipher text is obtained using Initialization Vector that is generated by the algorithm and is employed in the Decryption process to decrypt the cipher text to obtain the plain text. The working of the CBC is displayed as diagram beneath,

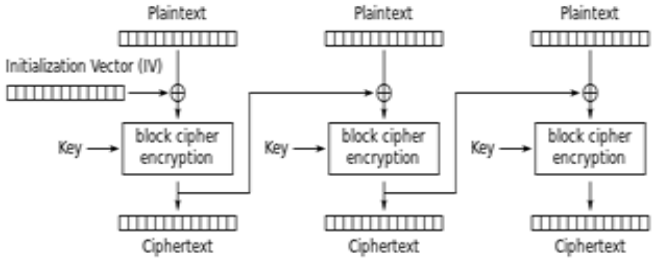

Figure 2.2 Cipher Block Chaining (CBC) mode Encryption

The above diagram 2.2 emphasizes the Encryption process of the plain text into un-intelligible format using CBC algorithm.

B Decryption Process

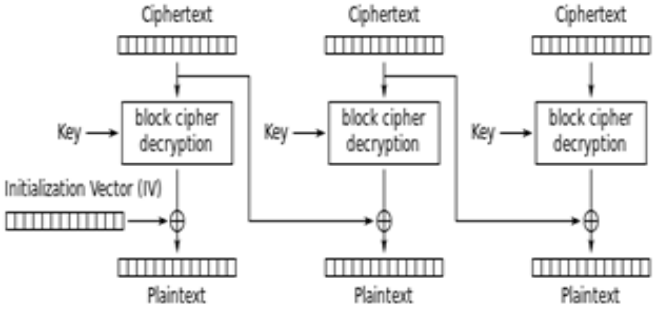

Figure 2.3 Cipher Block Chaining (CBC) mode Decryption

C Proposed System

In the above Figure: 2.3 the proposed system enables e-voting [13] for the citizens, providing security and privacy of the citizen's details. The

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

proposed system employs the block-chaining technique for the purpose of allocating a vast group of citizens. The block-chaining is applicable for dynamic purposes, where the blocks allocate and de-allocate in a dynamic manner. The framework request two different parameters, they are:

D Legitimate Voter Id

DOB associated with the registered voter id of the user.

These parameters then are subjected for verification and validation at the database server. The database server invokes the SMS Gateway API function that transmits a 6-digit One Time Password in a randomized fashion to the user's registered mobile number. The algorithm employed for the block-chaining is Cipher Block Chaining that is invoked at the provider end to encrypt the data and transmit the hashed value. The advantages of the proposed system are [17]:

Pervasive utility

Electronic – Voting

Fraudulent Detection

Dynamic Allocation

The framework is employed with dictionary containing of the following variables, they are:

Previous block – This stores the hash value of the previous block. The previous block hash value is generated using "hashlib" in the python. The SHA-256 hashing algorithm is used that provides a 256 bit hashed value as an output.

Transaction – This variable stores another dictionary of transaction related values in this case the

Voter Id

Date-of-Birth

One Time Password

In the below Figure: 2.4 thus the proposed system employs the SHA-256 algorithm [5] for the purpose of the hashing and generates a 256 bit output hashed value [19]. "c" here indicates encrypting process. Encrypting is enabled using SHA-256 algorithm.

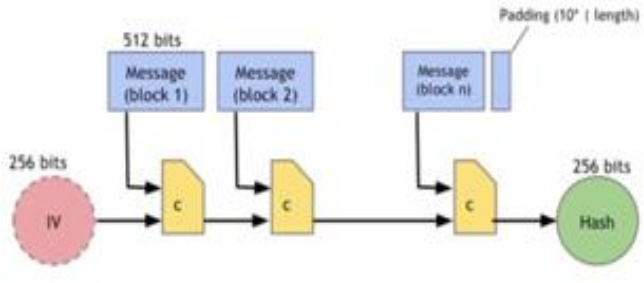

Figure 2.4 SHA-256 Hash function

E Implementation and Result

The proposed system is provided with the backend of Relational and Structured Database, this database is available with various details of the voters and their primary identification ie., Voter's ID. The service is implemented at the server supported with Django [18], WSGI and Nginx so that network is managed with load balancing and traffic control to avoid congestion.

The web service is provided with a form that request the user's voter's id and name along with their date-of-birth the Voter's Database is considered for reference in the backend, and an One Time Password is sent to the voter's id registered mobile number via SMS Gateway named TextLocal API [22]. The One Time Password is a randomized six-digit-length alphanumeric combination. The One-Time Password is encrypted with the voter's date-of-birth in order to promote the privacy and security of the user's credentials. In the below Figure: 2.6 represents User Interactive screen

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 8858 - 8865

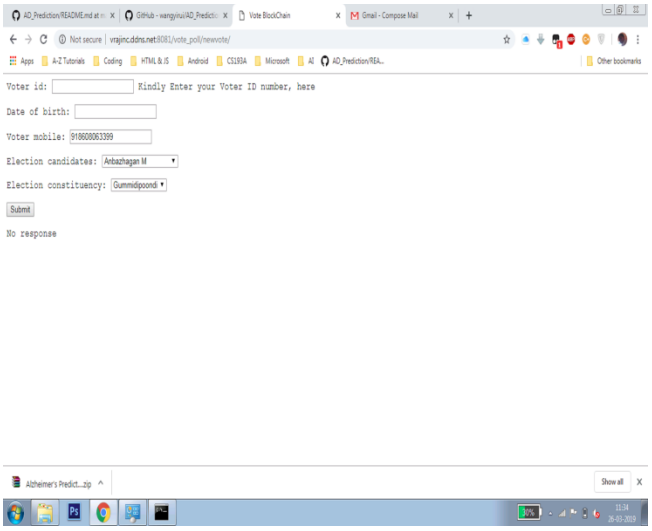

Figure 2.6 Users Interactive Screen

The response is accepted at the client's end as JSON object that is parsed and displayed the necessary information and the other information are abstracted. In case of wrong credentials, the message is notified to the customer with the update to report the corresponding activity carried out by the user/voter.

The sample Message that comprise of the One-Time-Password [11] is displayed beneath, the alphanumeric OTP generated is case-sensitive in order to improvise the efficiency of brute-force attack.

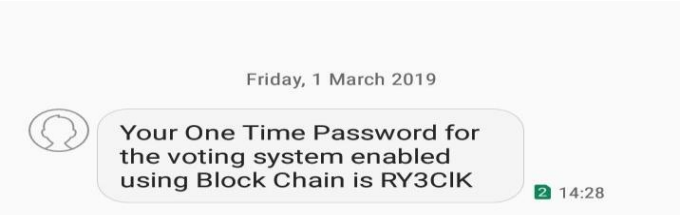

Figure 2.7 One Time Password generation

The above Figure: 2.7 after the successful completion of the e-voting the voter is replied to the voter's registered mobile number with their success report. After each and every vote, the block is appended in the block-chain system which consists of respective transaction result and details and further transaction are also attached with the respective block of the vote

III. ACKNOWLEDGEMENT

This work was supported by DST-FIST Programme No.SR/FST/College-110/2017, Government of India

REFERENCES

[1]. The "Leaderless, Block chain-Based Venture Capital Fund Raises $100 Million, And Counting", published with the Title of the book, that is stored as an archive the original on May 21 2016 by Morris, David Z.

[2]. The "A Venture Fund with Plenty of Virtual Capital, but No Capitalist", is the report that was published by the New York Times, authors are Popper, Nathan, which is archived on May 22 2016.

[3]. The repository named the "original-bitcoin" developed by Trottier, Leo and published on the Online development platform named github, which was archived from the original published on April 17 2016.

[4]. "The Truth AboutBlockchain", is the Title of the review published on Harvard Business Review by the Harvard University authors are Iansiti, Marco; Lakhani, Karim, which was archived from the original on January 18 2017.

[5]. "How to time-stamp a digital document" the Title of the journal proposed by Haber, Stuart; Stornetta, W. Scott, published by the Journal of Cryptology, with reference to the pages: 99–111, available at: https://link.springer.com/article/10.1007%2FBF00196791.

[6]. Chiraag Patel (2014-02-26). "Huntercoin is the World's First Peer to Peer Massively Multiplayer Online Cryptocurrency Game". Medici. Retrieved 2018-05-17.

[7]. "Move over Bitcoin, the blockchain is only just getting started" with the Title of the article published on Wired by Armstrong, Stephen, which was archived from the original on November 8 2016.

[8]. Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical

Computer Science. 1. Elsevier.
[9]. Biggs, Norman (2008). Codes: An introduction to Information Communication and Cryptography. Springer. p. 171.
[10]. ChristofPaar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.
[11]. Introduction to Modern Cryptography, with the Title of the book published by Katz, Jon; Lindell, Y at CRC Press, with a International Standard Book Number: ISBN 1-58488-551-3.
[12]. Saltman, Roy.EFFECTIVE USE OF COMPUTING TECHNOLOGY IN VOTE-TALLYING Archived 2016-02-11 at Wikiwix. NIST.
[13]. "How online voting works". usatoday.com. 10 March 2000.
[14]. Bochsler, Daniel (May 26, 2010). "Can Internet voting increase political participation?" (PDF). Centre for the Study of Imperfection in Democracies. Archived (PDF) from the original on September 18, 2016.
[15]. apleasant (2013-11-25). "E-voting Audits in Venezuela". www.ndi.org. Archived from the original on 2017-02-14. Retrieved 2017-02-13.
[16]. Grossman, Wendy M (30 April 2009). "Why machines are bad at counting votes". London: The Guardian. Archived from the original on 28 February 2014. Retrieved 2009-07-14.
[17]. Rubin, Avi (2002). "Security Considerations for Remote Electronic Voting over the Internet". Communications Policy and Information Technology: Promises, Problems, Prospects. MIT Press. p. 105. ISBN 978-0-262-03300-8. Archived from the original on 2018-05-10.
[18]. "3. Data model — Python 3.6.1 documentation". docs.python.org. Retrieved 2017-03-24.
[19]. Plain ASCII is a 7-bit character encoding, although it is often stored in 8-bit bytes with the highest-order bit always clear (zero). Therefore, for plain ASCII, the bytes have only 27 = 128 valid values, and the character translation table has only this many entries.
[20]. Knuth. "The Art of Computer Programming". Volume 3: "Sorting and Searching". Section "6.4. Hashing".
[21]. FAQ: General - Django documentation - Django". Retrieved 30 April 2016.
[22]. "Secure Blockchains for Dynamic Spectrum Access : A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access", with the Title of the journal published at IEEE Vehicular Technology Magazine, proposed by K. Kotobi, and S. G. Bilen, on 2018.
[23]. “Representational State Transfer”, with the Title of the Chapter of the book published on Architectural Styles and the Design of Network-based Software Architectures (Ph.D.). At University of California, Irvine, proposed by Fielding, Roy Thomas, the reference link associated with the Chapter-5 is :
https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm.