

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Online Voting System Using Blockchain

Mr.T.N.Prabhu¹, R. Navaneetha Kumar², P. R. Revant², S. Pandiarajan²

Assistant Professor (Sr. G), Department of Information Technology, Sri Ramakrishna Engineering College,
Vattamalaipalayam, Coimbatore, Tamilnadu, India¹

U.G Student, Department of Information Technology, Sri Ramakrishna Engineering College, Vattamalaipalayam,
Coimbatore, Tamilnadu, India²

ABSTRACT: Democratic voting is a crucial and serious event in any country. The most common way in which a country votes is through a paper based system, but is it not time to bring voting into the 21st century of modern technology? Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when voting using a machine in a polling station, and i-voting when using a web browser. Security of digital voting is always the biggest concern when considering to implement a digital voting system. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of block chains. Block chain technology originates from the underlying architectural design of the crypto currency bit coin. It is a form of distributed database where records take the form of transaction. A block is a collection of these transactions. With the use of block chains a secure and robust system for 4 digital voting can be devised. This report outlines our idea of how block chain technology could be used to implement a secure digital voting system.

KEYWORDS: Online voting, Election, Candidate, Voters, Registration, Results.

I. INTRODUCTION

Democratic voting is a crucial and serious event in any country. Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. Security of digital voting is always the biggest concern. One way the security issues can be potentially solved is through the technology of blockchains. This report outlines the idea of how blockchain technology could be used to implement a secure digital voting system.

II. RELATED WORK

A number of digital voting systems are currently in use in countries around the world. It is a method for the classification of both linear and nonlinear data. Estonia has had electronic voting since 2005 and in 2007 was the first country in the world to allow online voting.

The bases of this system is the national ID card that all Estonian citizens are given. These cards contain encrypted files that identify the owner and allows the owner to carry out a number of online and electronic activities including online banking services, digitally signing documents, access their information on government databases.

III. PROJECT DESCRIPTION

In our project we use a algorithm namely SHA 256 (secure hashing algorithm). There are many cryptographic algorithms you can choose from, however SHA256 fits just fine for this example. We can import `java.security.MessageDigest`; to get access to the SHA256 algorithm. Hash = Digital Signature. Each block doesn't just contain the hash of the block before it, but its own hash is in part, calculated from the previous hash. If the previous block's data is changed then the previous block's hash will change (since it is calculated in part, by the data) in turn

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

affecting all the hashes of the blocks there after. Calculating and comparing the hashes allow us to see if a blockchain is invalid.

IV. BLOCK CHAIN

Blockchain is the backbone Technology of Digital CryptoCurrencyBitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by the majority of participants of the system. It contains every single record of each transaction. BitCoin is the most popular cryptocurrency an example of the blockchain. The bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through digital signature.

There is no Central Server or System which keeps the data of Blockchain. The data is distributed over Millions of Computers around the world which are connected with the Blockchain. This system allows Notarization of Data as it is present on every Node and is publicly verifiable. A block is a data structure that contains all the necessary metadata about the block(Block Header) itself and contains transactions. The first block in a blockchain is called the genesis block.

Block chain can be defined as a chain of the block that contains information. The technique is intended to timestamp digital documents so that it's not possible to backdate them or temper them. The block chain is used for the secure transfer of items like money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Once a data is recorded inside a block chain, it is very difficult to change it. Block chains could not be run without the Internet. A node is a computer connected to the Blockchain Network. A chain of blocks which contain some metadata about the block, some transactions and joined to the previous block by the previous block's hash value.

Node gets connected with Blockchain using the client. Client helps in validating and propagates transaction on to the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a transaction in return for an incentive is called Miners.

V. BIT COIN

Bitcoin transactions are digitally signed for security. Bitcoin, the decentralized network, allows users to transact directly, peer to peer, without a middle man to manage the exchange of funds. Bitcoin, the decentralized network, allows users to transact directly, peer to peer, without a middle man to manage the exchange of funds. Everyone on the network gets to know about a transaction. A transaction contains 3 pieces of information. The first part contains the bitcoin wallet address of the sender, the second part contains the amount that has been sent, and the third part contains the bitcoin wallet address of the recipient. A bitcoin can also be considered as an invisible currency with only the transaction records between different addresses. Every transaction ever made using Bitcoin is stored in a public ledger called a Blockchain. The digital asset, bitcoin, is used like other assets in exchange for goods and services. Unlike traditional currencies and assets, bitcoin is easily portable, divisible, and irreversible. The digital asset, bitcoin, is used like other assets in exchange for goods and services. Unlike traditional currencies and assets, bitcoin is easily portable, divisible, and irreversible.

There are a number of currencies in this world used for trading amenities. Rupee, Dollar, Pound Euro and Yen are some of them. These are printed currencies and coins and you might be having one of these in your wallet. But bitcoin is a currency you can not touch, you can not see but you can efficiently use to trade amenities. It is an electronically stored currency. It can be stored in your mobiles, computers or any storage media as a virtual currency. Bitcoin is an innovative and digital payment system. It is an example of a cryptocurrency and the next big thing in finance.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

VI. CRYPTOGRAPHIC HASH ALGORITHM

SHA-256 stands for Secure Hash Algorithm – 256 bit and is a type of hash function commonly used in Blockchain. A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. It's like a formula or algorithm which takes the input data and turns it into an output of a fixed length, which represents the fingerprint of the data. A cryptographic hash (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. See [below](#) for the source code.

The input data can literally be any data, whether it's the entire Encyclopedia Britannica, or just the number '1'. A hash function will give the same hash for the same input always no matter when, where and how you run the algorithm. Equally interestingly, if even one character in the input text or data is changed, the output hash will change. Also, a hash function is a one-way function, thus it is impossible to generate back the input data from its hash. So, you can go from the input data to the hash but not from the hash to the input data. **SHA-256** is a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. In this case, it is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. It is a modified version of SHA1, which in turn is a modified SHA0. All three are now broken, to some extent. **SHA-256** is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash. Hashing algorithms are used in all sorts of ways – they are used for storing passwords, in computer vision, in databases, etc. There are hundreds of hashing algorithms out there and they all have specific purposes – some are optimized for certain types of data, others are for speed, security, etc. For the sake of today's discussion, all we care about are the SHA algorithms. SHA stands for Secure Hashing Algorithm – its name gives away its purpose – it's for cryptographic security. If you only take away one thing from this section, it should be: cryptographic hash algorithms produce irreversible and unique hashes. Irreversible meaning that if you only had the hash you couldn't use that to figure out what the original piece of data was, therefore allowing the original data to remain secure and unknown. Unique meaning that two different pieces of data can never produce the same hash. The fundamental difference is that while encryption is a two way function (given the key) hash is only a one way function: given some data you can compute the hash, given the hash it is difficult (and mathematically impossible) to have the data back. It is mathematically impossible to find the data from the hash because typically a hash function has a small codomain (for example 256bit for SHA256) but a big domain (you can hash any string), so there will be collisions: different strings with the same hash. For this reason if your password is saved in a hashed form then there exist infinite password (but they can be very long) that unlocks your account. The good news is that collisions are rare when you use cryptographic hash functions, so your account is still safe. SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of $512 = 16 \times 32$ bits, each block requiring 64 rounds.

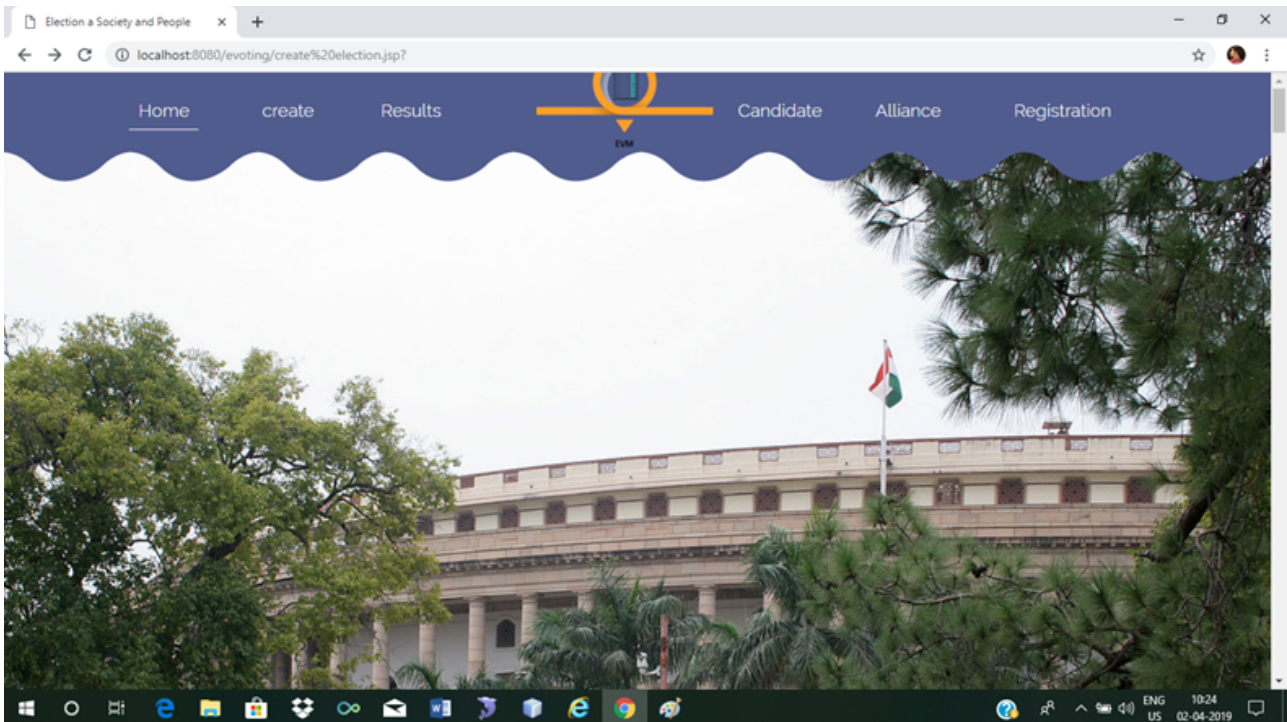
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

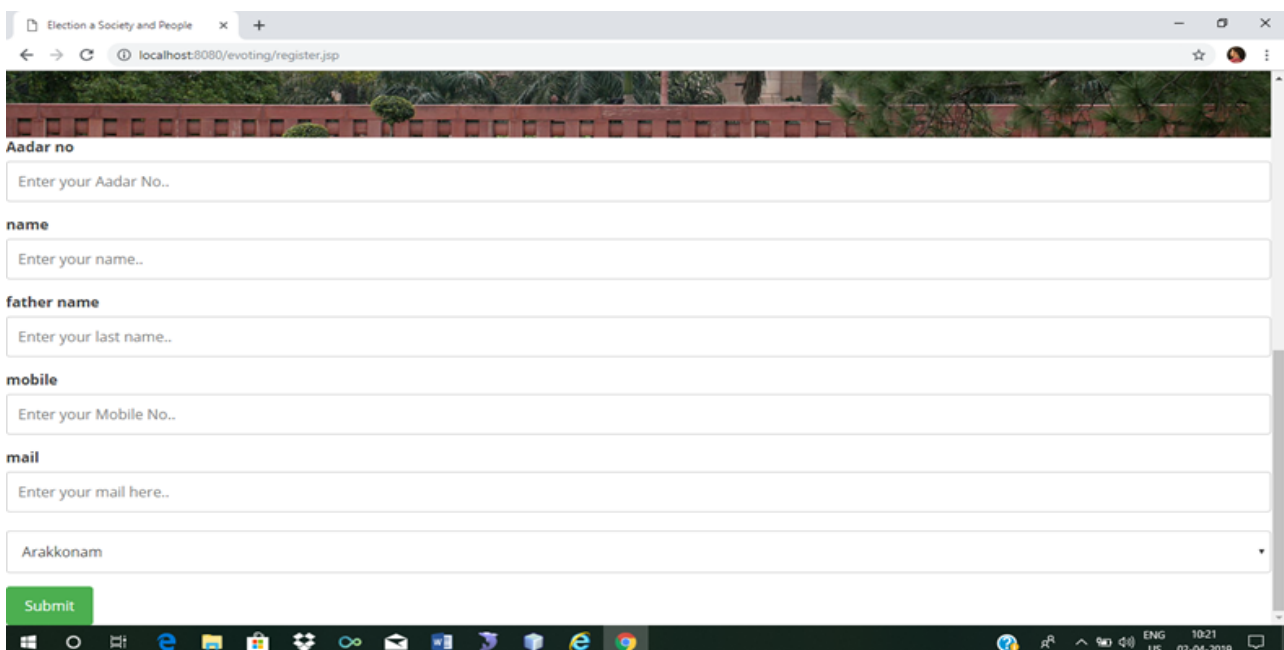
Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

VII. EXPERIMENTAL OUTPUTS



(a) Online Voting System



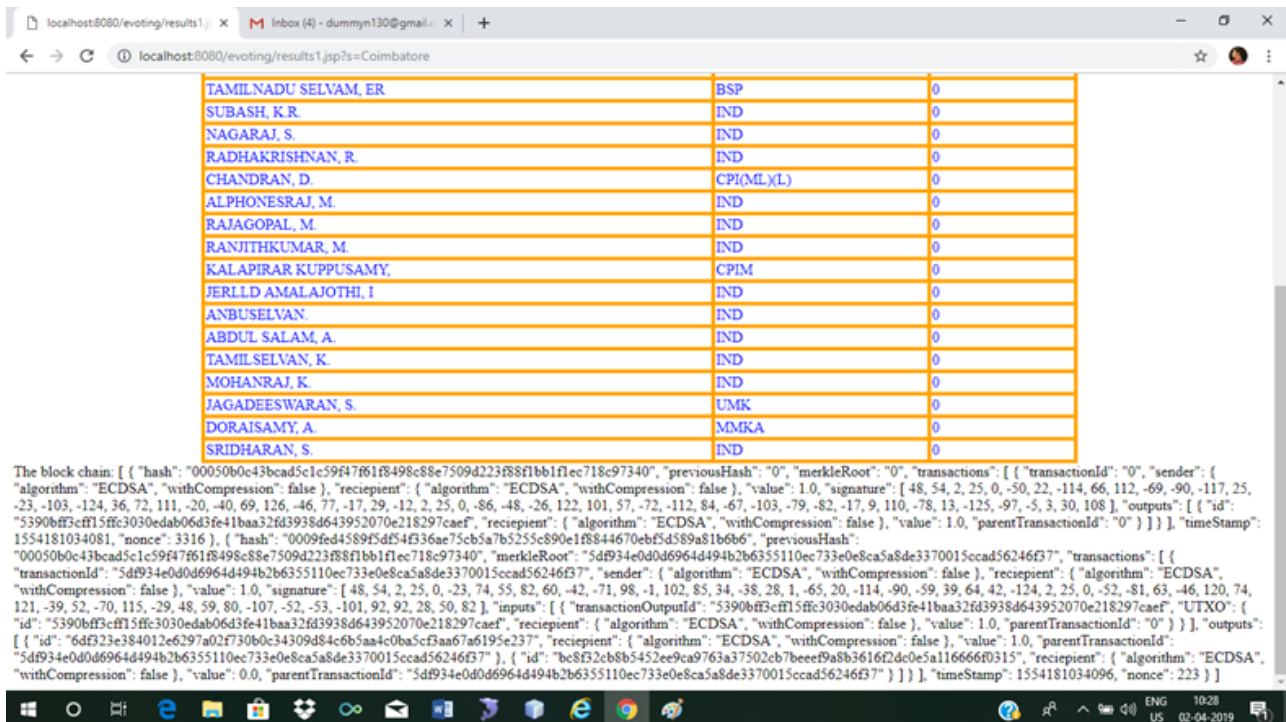
(b) Voters Registration Form

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019



TAMILNADU SELVAM, ER	BSP	0
SUBASH, K.R.	IND	0
NAGARAJ, S.	IND	0
RADHAKRISHNAN, R.	IND	0
CHANDRAN, D.	CPI(ML)(L)	0
ALPHONESRAJ, M.	IND	0
RAJAGOPAL, M.	IND	0
RANJITHKUMAR, M.	IND	0
KALAPIRAR KUPPUSAMY,	CPIM	0
JERLID AMALAJOTHI, I	IND	0
ANBUSELVAN,	IND	0
ABDUL SALAM, A.	IND	0
TAMILSELVAN, K.	IND	0
MOHANRAJ, K.	IND	0
JAGADEESWARAN, S.	UMK	0
DORAISAMY, A.	MMKA	0
SRIDHARAN, S.	IND	0

The block chain: [{ "hash": "00050b0c43bcad5c1c59f4761f8498e88e7509d223f88f1bb1fec718c97340", "previousHash": "0", "merkleRoot": "0", "transactions": [{ "transactionId": "0", "sender": { "algorithm": "ECDSA", "withCompression": false }, "recipient": { "algorithm": "ECDSA", "withCompression": false }, "value": 1.0, "signature": [48, 54, 2, 25, 0, -50, 22, -114, 66, 112, -69, -90, -117, 25, -23, -103, -124, 36, 72, 111, -20, -40, 69, 126, -46, 77, -17, 29, -12, 2, 25, 0, -86, -48, -26, 122, 101, 57, -72, -112, 84, -67, -103, -79, -82, -17, 9, 110, -78, 13, -125, -97, -5, 3, 30, 108], "outputs": [{ "id": "5390bff3cfl15ffc3030edab06d3fe41baa32fd3938d643952070e218297caef", "recipient": { "algorithm": "ECDSA", "withCompression": false }, "value": 1.0, "parentTransactionId": "0" }] }, { "timeStamp": 1554181034081, "nonce": 3316 }, { "hash": "0009fed4589f5d54f336ae75cb5a7b5255c890e1f8844670ebf5d389a81b6b6", "previousHash": "00050b0c43bcad5c1c59f4761f8498e88e7509d223f88f1bb1fec718c97340", "merkleRoot": "5df934e0d0d6964d494b2b6355110ec733e0e8ca5a8de3370015ccad56246f37", "transactions": [{ "transactionId": "0", "sender": { "algorithm": "ECDSA", "withCompression": false }, "recipient": { "algorithm": "ECDSA", "withCompression": false }, "value": 1.0, "signature": [48, 54, 2, 25, 0, -23, 74, 55, 82, 60, -42, -71, 98, -1, 102, 85, 34, -38, 28, 1, -65, 20, -114, -90, -59, 39, 64, 42, -124, 2, 25, 0, -52, -81, 63, -46, 120, 74, 121, -39, 52, -70, 115, -29, 48, 59, 80, -107, -52, -53, -101, 92, 92, 28, 50, 82], "inputs": [{ "transactionOutputId": "5390bff3cfl15ffc3030edab06d3fe41baa32fd3938d643952070e218297caef", "recipient": { "algorithm": "ECDSA", "withCompression": false }, "value": 1.0, "parentTransactionId": "0" }] }, { "outputs": [{ "id": "6df323e384012e6297a02f730b0c34309d84c6b5aa4c0ba5c3aa67a6195e237", "recipient": { "algorithm": "ECDSA", "withCompression": false }, "value": 1.0, "parentTransactionId": "5df934e0d0d6964d494b2b6355110ec733e0e8ca5a8de3370015ccad56246f37" }, { "id": "bc8f32cb8b5452ee9ca9763a37502eb7beef9a8b36162de0e5a116666f0315", "recipient": { "algorithm": "ECDSA", "withCompression": false }, "value": 0.0, "parentTransactionId": "5df934e0d0d6964d494b2b6355110ec733e0e8ca5a8de3370015ccad56246f37" }] }, { "timeStamp": 1554181034096, "nonce": 223 }]]

(c)Result and Block Chain

VII. CONCLUSION

The project concludes that by using block chain we can manage the voting directory and, we can avoid failures of voting list and fraud detection. The block manages the has values and dataset. Thus, the report outlines the idea of how blockchain technology could be used to implement a secure digital voting system.

REFERENCES

- [1] Gartner, "Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017", available at <http://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/>.
- [2] P. Frøystad, and J. Holm, "Blockchain: Powering the Internet of Value", EVRY Labs, 2016.
- [3] E. Mengelkamp, J. S. Gärtner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid", Applied Energy, Vol. 210, 2018, pp. 870-880.
- [4] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains", IEEE Transactions on Industrial Informatics, Vol. 13, Issue 6, 2017, pp. 3154-3164.
- [5] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, no. 6, pp. 539-556, 2002.
- [6] R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382-392.
- [7] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574-575. [Online]. Available: <http://doi.acm.org/10.1145/3085228.3085263>
- [8] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.
- [9] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357-375.
- [10] BitCongress. Control the world from your phone. [Online]. Available: <http://www.bitcongress.org/BitCongress Whitepaper.pdf>