Visual Cryptography as Authentication for Secure E-voting using Blockchain

Durande Sneha, Mohite Kamini, Sarode Haridas*
Department of Computer Science and Engineering
SVPM's college of engineering Malegaon (bk)
Corresponding author's email id: *harisarode007@gmail.com**
DOI: *http://doi.org/ 10.5281/zenodo.2647711*

Abstract

Increasing digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still wide spread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solution, because it embraces a decentralized system and the entire database is owned by many users. Block chain itself has been used in the Bit coin system known as the decentralized Bank system. By adopting blockchain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bit coin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.

This is a project with the objective to develop a basic website where a consumer is provided with a shopping cart website.

This document will discuss each of the underlying technologies to create and implement an e-commerce website.

Keywords: *Blockchain, Decentralized database, Bit coin, Visual cryptography etc.*

INTRODUCTION

A blockchain is list of records, called blocks, which are join using concept of cryptography. A cryptographic hash of the previous block, a timestamp, and transaction data are the main content of each and every block. Basically a blockchain is developed for resistant to modification of the data. It is an open, distributed system which keeps record of transactions between two parties. Also it preserves verifiable record in permanent way. Because of distributed system a blockchain is managed by a peer-to-peer network and add new block by validating new blocks in blockchain. Once record is stored the data in any of block in blockchain cannot be changed without permission of all subsequent blocks, which requires unity of the network majority.

Blockchain was coined by Satoshi Nakamoto in 2008 to keep as the public transaction of the crypto currency bitcoin. The research of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted third party or central server. Private blockchains have been proposed for business use. A blockchain is a distributed, immutable, incontrovertible, public ledger.

This blockchain technology has following four main features:

(i) The ledger exists in many different places therefore no single point of failure in distributed ledger.

(ii) Distributed control over distributed leger for appending new transactions to the chain.

(iii) For adding new block to the chain must reference the previous version of the block in blockchain, make immutable leger.

(iv) A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

In every democracy, the security of an election is a matter of national security. The computer security field has for a decade studied the possibilities of electronic voting systems, with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. From the dawn of democratically electing candidates, the voting system has been based on pen and paper. Replacing the traditional pen and paper scheme with a new election scheme that is why e-voting using blockchain

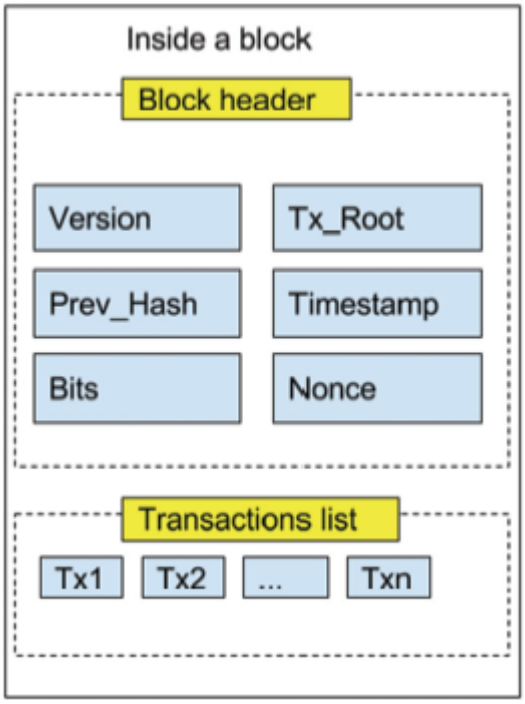


Figure 1 Block Structure

I. prev_hash: This field can be known as a reference to parents, which is a link of a block to its previous one in the chain. All the information inside the previous block will be inputted to a hash function to get a value, and then this value will be assigned to the field prev_hashin the new block. In Bitcoin, a 256-bit hash function is used to get this value

II. **Timestamp:** The time when the block was found.

III. **Tx_root:** This field, which is also known as the Merkle root contains the hash value of all validated transactions of the block. As seen from the example in Fig. 2, all the transactions are hashed into a hash value; then they combine with each other pair-by-pair, and are inputted to another hash function. This work is repeated, until there is only a single entity, which stands for the Merkle root.

IV. **Version:** This field contains the protocol version used by the node proposing the block to the chain.

V. **Nonce:** This field is used in PoW, which proves the efforts that a node has paid for getting the right to append his block to the chain. This field will be presented in the next section.

VI. **Bits:** This field indicates the difficulty level of the PoW.

MOTIVATION

Motivation behind this work is to provide the secure, fast, reliable and transparent e-voting system. Blockchain is highly secure and recent technology which based on decentralized e-voting protocol, without the existence of a trusted third party. In previous voting system the voter has problem like:

1) Remote voting is not possible.
2) In EVM based voting the manual ink system to avoid fake voting
3) Election results are centralized.
4) Lack of transparency in EVM results.

LITERATURE SURVEY

There is currently a number of research work performed in the area of bringing transparency in E-voting system.

An E-voting Protocol Based on Blockchain, Yi Liu and Qi Wang based on the blockchain technology propose a decentralized e-voting protocol, to provide possible extension and improvement in voting scenario without the existence of a trusted third party.

Crypto-voting, a Blockchain based e-Voting System, Francesco Fusco, Maria Ilaria Lunes, Filippo Eros Pani and Andrea Pinna

The purpose of this study is the presentation and the definition of a new e-voting system named Crypto-voting. We base this solution upon the Shamirs secret sharing approach, using blockchain technology implement new e-voting system. This e-voting system named Crypto-voting with no middleman.

Zerocash: Decentralized Anonymous Payments from Bitcoin, Eli Ben Sasson ; Alessandro Chiesa ; Christina Garman ; Matthew Green ; Ian Miers ; Eran Tromer ; MadarsVirza,2014 IEEE Symposium on Security and Privacy, IEEE

Bit coin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bit coin cannot offer strong privacy guarantees, Results leverage recent advances in zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). First, we formulate and construct decentralized anonymous payment schemes (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's security. Second, we build

Zero cash, a practical instantiation of our DAP scheme construction.

Electronic Voting Using Block-Chain Service (Jushua I James)

In this beyond financial transactions blockchain technology is used to audit the integrity of the transaction. The focus on this paper is the potential availability of block-chain technology of other transactional uses.

SHARVOT: Secret SHARe-Based VOTing on the Blockchain,Silvia Bartolucci ; Pauline Bernat ; Daniel Joseph, 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), IEEE.

Nowadays growing interest in using online technologies to design protocols for secure electronic voting but main challenges are vote privacy, anonymity, ballot irrevocability and transparency throughout the vote counting process. The introduction of the blockchain as a basis for crypto currency protocols provides for the exploitation of the immutability and transparency properties of these distributed ledgers. This blockchain concept possibly used to implement a secure and fair voting system. In particular, in this introduce a secret share-based voting system on the blockchain, the so-called SHARVOT protocol1.

GOALS & OBJECTIVES

- To develop E-Voting System Using Visual Cryptography (VC)
- To provide a flexibility to allow casting vote from any remote place
- To provide confidentiality by applying appropriate security measures by visual cryptography.

PROPOSE SYSTEM

In this proposed system there are two working modules used

1) Administrator
2) Voter

Administrator:

Here administrator is the Election Commission of India. Who is responsible for the different activities in election

- Uploading Voter information
- Verifying Voter information
- Uploading Candidate Information
- Generating, broadcasting the ballot paper to voter
- Date/ Time Sets by Election Commission of India

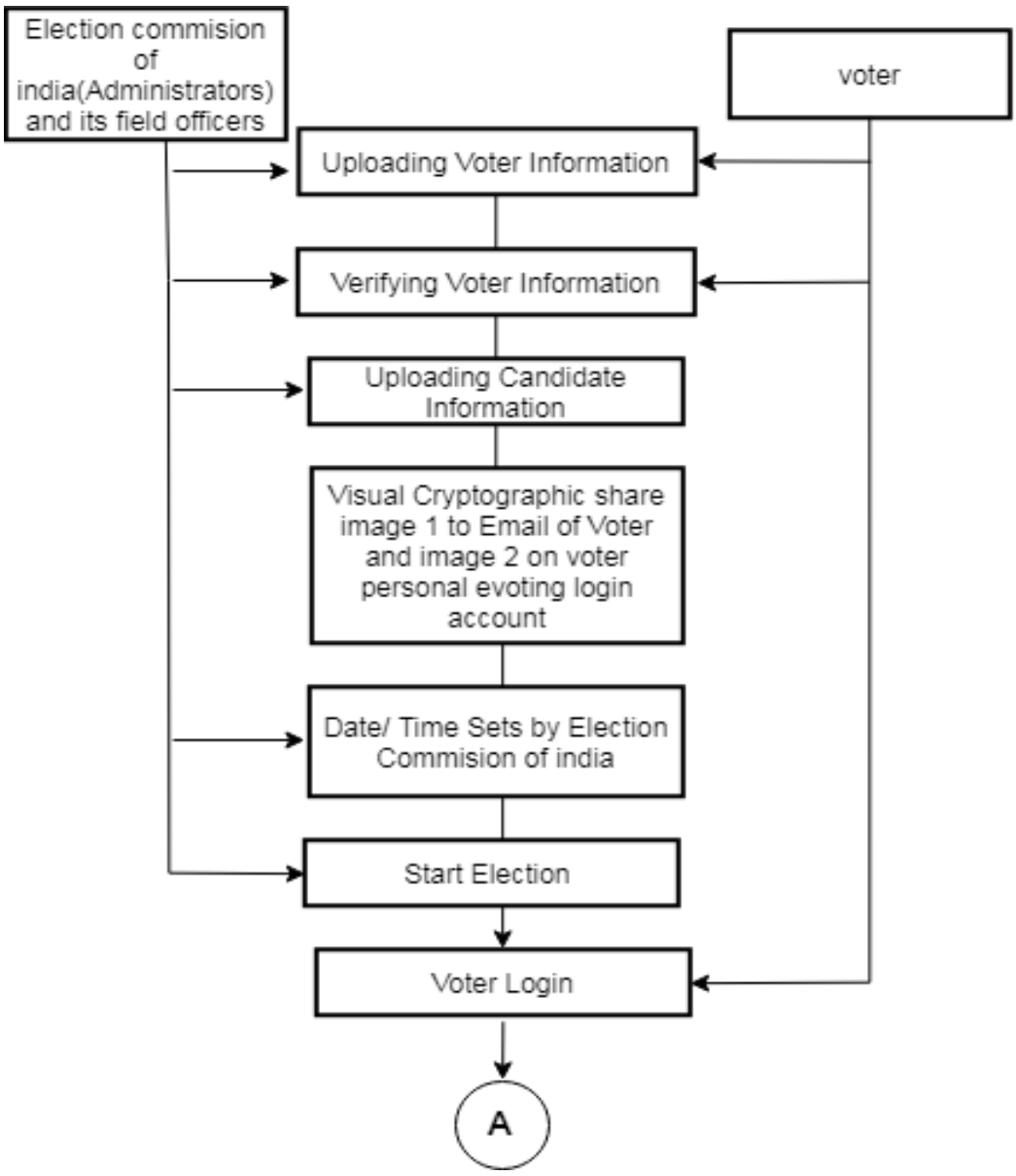
- Start Election
- Declaring results

Voter:

- Registration
- Uploading Self Information
- Verifying Information
- Login
- Select candidate from ballot paper

Architectural Design

The proposed architecture design contain the part which are working sequentially as figure shows the part of System architecture is the design of the whole system architecture.



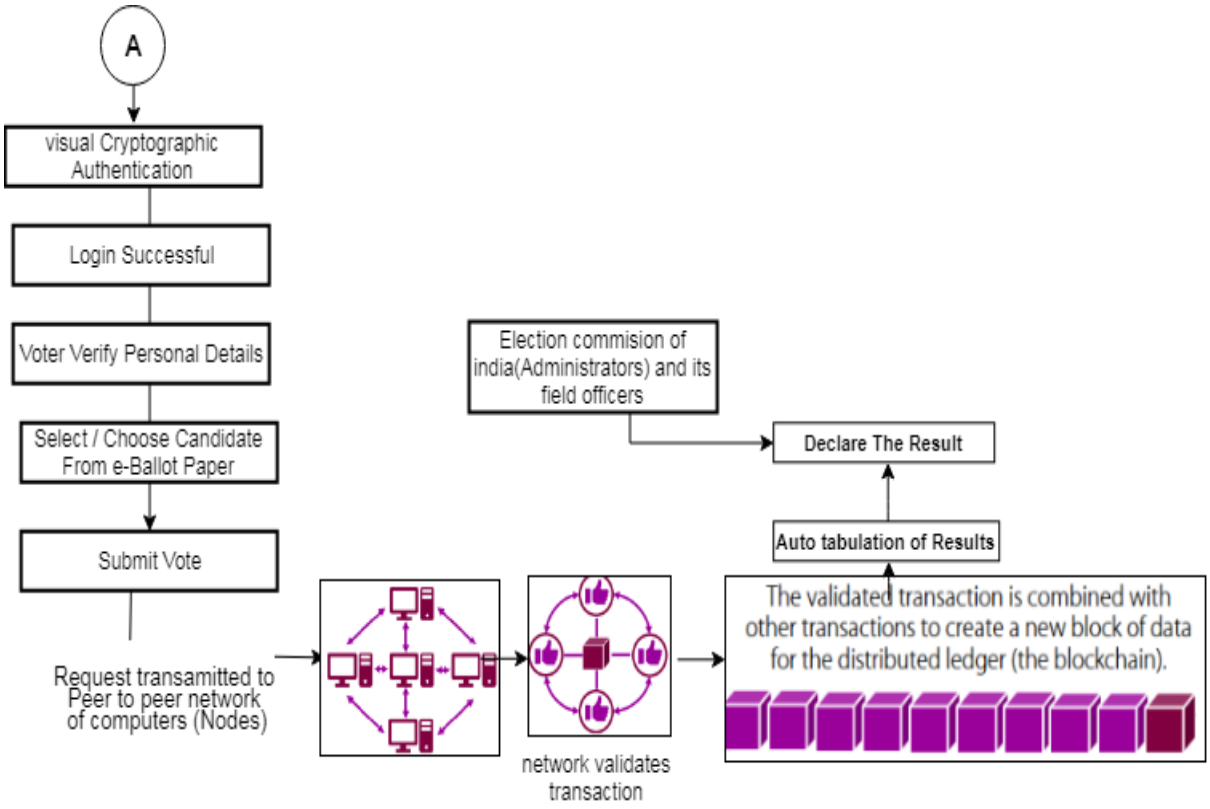


Fig2. Detailed System Architecture Data Flow

In the e-voting system using block chain is made up of peer to peer network. Voter is the person who is the user who want cast his/her votes in the election using e-voting system. Administrator has control only upto the starting of the election. Election commission first provides the interface to the client for uploading their information after uploading information by user/voter. Election commission verify that information give right to cast vote to user.

When election days start election commission upload candidate's information and set time and date of election on election day election commission start the election that time voter login to the system by providing their Aadhar card number as username and for password it request a otp that generate from the system by visual cryptographic authentication system. In VC the image is provide as password but that image is breaks down in two share one share is provide by system itself and half part is send on voter Gmail after downloading that half part when voter provide to system voters personal details get verified. After voter get successfully verify then can select or choose candidate from e-Ballot paper and cast their vote.

After submitting vote these request transmitted to peer to peer network of computer of authorized nodes, then each node validate the block of vote information by doing all arithmetic calculations. When validated transaction is combined to other previously validated transaction and form a chain of all validated block

When election time over automatic result is prepared and declares the result system itself.

FUTURE SCOPE

In future extension, we aim to instead of using visual cryptography technique for voter authentication other technique to authenticate the voter. Future work will also include the more secure encryption schemes to be used in our models.

CONCLUSION

In this project, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. By comparing to e-voting system, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost-time efficient election scheme, also increasing the security issue of the today's scheme and offer new possibilities of transparency. Our election scheme allows individual voters to vote from remote place so that voter guaranteeing that each individual voters vote is counted from, which could potentially increase voter turnout.

REFERENCES

I. Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/ elections/ voting-systems/oversight/ top-bottom-review/.

II. Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/secure-vote-today.

III. TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain/

IV. Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

V. Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/ wiki/White-Paper.

VI. Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online]. Available at: https://nca.tandfonline.com/doi/abs /10.1080/ 13183222.2015.1017264#.Wr0zCn Vl8YR

VII. Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). Anonymous voting by two-round public discussion. Available at: http://homepages.cs.ncl.ac. uk/feng.hao/files/OpenVote_IET.p df

VIII. Feng Hao and Piotr Zielinski. A 2-Round Anonymous Veto Protocol Available at: http://homepages.cs.ncl.ac.uk/feng. hao/files/av_net.pdf.

IX. The Dining Cryptographers Problem: Unconditional Sender and Recipient Intractability. Available at: https://users.ece.cmu.edu/~{}adria n/ 731-sp04/readings/dcnets.html.

X. Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy Available at: https://eprint.iacr.org/2017/110.pdf .

XI. Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme Available at: http://www.win.tue.nl/~berry/paper s/euro97.pdf

XII. Jonathan Alexander, Steven Landers and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at: https://netvote. io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf

XIII. Agora (2017). Agora: Bringing our voting systems into the 21st

century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

XIV. Kirill Nikitin, Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, Justin Cappos and Bryan Ford (2017). CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds Available at: https://www.usenix. org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf

XV. Alin Tomescu and Srinivas Devadas(2017). Catena: Efficient No equivocation ia Bitcoin Available at: https://people.csail.mit.edu/alinush/papers/catena-sp2017.pdf

XVI. Michael del Castillo (2018). Sierra Leone Secretly Holds First Blockchain-Audited Presidential Vote Available at: https://www.coindesk.com/ sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote/

XVII. Ethereum Blog. (2018). On Public and Private Blockchains - Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

XVIII. Bitfury.com. (2018). Digital Assets on Public Blockchains Available at: http://bitfury.com/content/5-white-papers-research/bitfury-digital_ ssets_on_public_blockchains-1.pdf

XIX. Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A Decentralized

Cite this Article

Durande Sneha, Mohite Kamini, Sarode Haridas (2019). **Visual Cryptography as Authentication for Secure E-voting using Blockchain** Journal of Computer Aided Parallel Programming, 4(1),19-28

http://doi.org/ 10.5281/zenodo.2647711