SECURE ONLINE VOTING SYSTEM USING BLOCK CHAIN

A. Udayaprakash , G.muthumanikandeshwaran

Department of Computer Science Engineering ,Prince Shri Venkateshwara Padmavathy Engineering College

Abstract

Distributed wireless networks perform critical network functions such as fault-tolerant data fusion cooperative sensing, and reaching consensus in voting system . The delay overhead of voting can be prohibitive when numerous participants have to share the post in sequence, making it impractical for time-critical applications. We propose a fast and secure Block chain voting scheme called Block chain Voting System , which significantly reduces the delay for collecting and tallying votes. In Block chain voting system(BVS) , Voters transmit their votes simultaneously by exploiting the blocks in online. Votes are realized by injecting energy to pre-assigned blocks. BVS is secure against hackers and third parties , Security is achieved by employing cryptography-based authentication and message integrity schemes. Evaluating the voting robustness as a function of Block parameters. the practical implementation challenges are multi-device frequency and time synchronization.

Keywords - *Block chain voting system , robustness , cryptography , consensus , prohibitive , data fusion .*

I. INTRODUCTION

Block chain is a growing list of records called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data . A block chain is resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way . Block chain usually managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Block chains may be considered secure by design and high fault tolerant system . Blockchain technology allows for fast, secure, and transparent peer-to-peer transfer of digital goods that include money and intellectual property. In crypto coin mining and investing, it's an important topic to understand. One of the most talked about and misunderstood topics in recent times, blockchain technology is completely overhauling the way digital transactions are conducted and could eventually change the way several industries conduct their daily business.

Two words that have rapidly become part of the mainstream vernacular are bitcoin and block chain. While they are related, these terms refer to two different things. Bitcoin is a form of virtual currency, more commonly known as crypto currency , which is decentralized and allows users to exchange money without the need for a third-party. All bitcoin transactions are logged and made available in a public ledger to ensure their authenticity and prevent fraud. The underlying technology that facilitates these transactions and eliminates the need for an intermediary is the block chain.

One of block chain's main benefits lies in its transparency, as the ledger functions as a living, breathing chronicle of all peer-to-peer transactions that occur. Each time a transaction takes place, such as when one party sends bitcoin directly to another, the details of that deal including its source, destination, and timestamp are added to a block. On an individual basis, miners are computers that are configured to use their GPU or CPU cycles to solve complex mathematical problems, passing the block's data through a hashing algorithm until a solution is found. When the problems are solved, the block and all of its respective transactions are verified as legitimate. Rewards bitcoin or some other currency are then divvied up among the computer or computers that contributed to the successful hash.

When the transactions within a block are deemed valid, they are attached to the most recently verified block in the chain, creating a sequential ledger which is viewable by anyone.

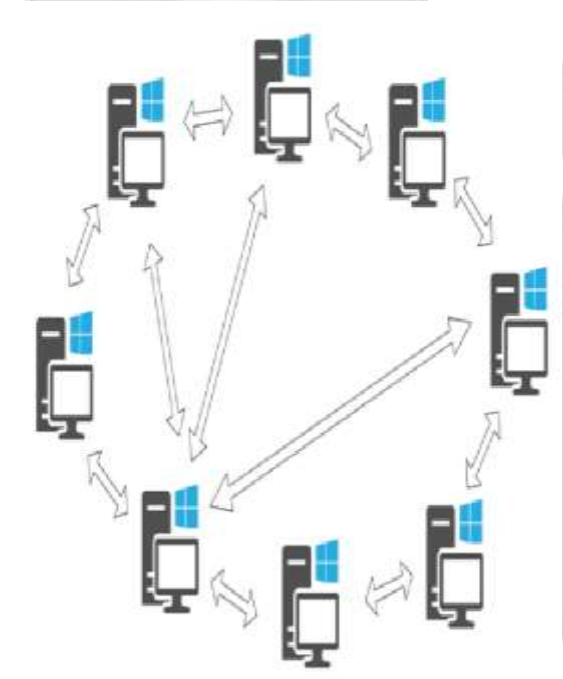
This process continues in perpetuity, expanding on the block chain's contents and providing a public record that can be trusted. In addition to being constantly updated, the chain and all of its blocks are distributed across the network to a large number of machines. This ensures that the latest version of this decentralized ledger exists virtually everywhere, making it almost impossible to forge.

The block chain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the block chain.

Information held on a block chain exists as a shared and continually reconciled database. This is a way of using the network that has obvious benefits .

Peer-to-peer connectivity over the internet has existed for some time in a number of formats, allowing for the distribution of digital assets directly from one person or business to another. The behaviour of the bitcoin block chain is the perfect example to answer this question. Pretend for a moment that there was no block chain in place and that you had one bitcoin token in your possession with its own unique



.

Now, say you wanted to buy a new television from a business that accepts cryptocurrency, and that shiny new TV happens to cost one bitcoin . Unfortunately, you also need to pay back your friend for the bitcoin which you borrowed from him last month. In theory, without the block chain in place, what's to stop you from transferring that same digital token to both your buddy and to the electronics store?

This dishonest practice is called double-spending, and it's one of the main reasons why peer-to-peer digital transactions have never really caught on until now. With block chain, which not only distributes a public record of all transactions but confirms a block before each of its individual transactions can be finalized, the possibility of this fraudulent activity is essentially wiped out.

In the past, intermediaries such as banks and payment processors validated these transactions to make sure that everything was on the up and up. Block chain technology lets a user to transfer digital assets from point A to point B, taking comfort in the fact that reliable checks and balances are in place.

The ability for anyone to view a public block chain such as the one associated with virtual currencies is a key factor in why the technology works as well as it does. The easiest way to peruse this distributed database is through a block explorer, typically hosted on a free-to-use website such as Blockchain.info.

Most block chain explorers are heavily indexed and easily searchable, allowing you to locate transactions in a number of different ways including by IP address, block hash, or other relevant data points.

Block chain has come to the forefront of many discussions because of its role in the distribution of cryptocurrencies like bitcoin. In the long run, these digital cash transactions may end up being a small part of blockchain technology's overall footprint on the world as a whole and the way assets are transferred online.

The possibilities for blockchain implementation seem endless, as its underlying technology can be leveraged in many fields to perform a number of important tasks such as:

- Executing contracts
- Safely buying and selling intellectual property
- Distributing important medical information
- Ensuring that voting in elections is incorruptible
- Instant results
- Reliable system
- No data centralization

World society has just begun to scratch the surface of block chain applications. New potential uses for block chain are being discovered on a regular basis. Private block chains will allow companies to revolutionize their own internal processes, while public, open-source variations will continue to change the way people handle business in their daily lives.

Distributed wireless networks perform critical network functions such as fault-tolerant data fusion, cooperative sensing, and reaching consensus in voting system. They use fusion centre for sending messages . Voting is implemented by sending messages to a fusion center or via direct message exchange between participants. However, the delay overhead of message-based voting can be prohibitive when numerous participants have to share the wireless channel in sequence, making it impractical for time-critical applications .

Blockchain and the Internet of Things (IoT) are key technologies that will have a huge impact in the next 10 years for companies in the industrial market. This article describes how these two technologies will improve efficiencies, provide new business opportunities, address regulatory requirements, and improve transparency and visibility.

Supply chain use cases are the most common application of block chain for solving real business problems due to the lack of visibility of shipment data for product or component information as the shipment moves through the supply chain.

Shipment delays are often due to intermediaries within the supply chain whose role is approval of paperwork associated with the shipments. Paperwork has a tendency to get misplaced or lost, or is awaiting processing as the piles of paperwork grow. What if this paperwork could be digitized on the block chain? The need for these types of intermediaries could be removed from the supply chain.

The block chain would capture key shipment data emitted from IoT devices attached to products or components as the shipment moves from source to destination.

The IoT platform would invoke a transaction for the block chain that contains the shipment container location and timestamp.

Block chain is a technology that uses community validation to keep synchronized the content of ledgers replicated across multiple users. Although block chain derives its origins from technologies introduced decades ago, it has gained popularity with Bitcoin . Bitcoin’s block chain is a decentralized peer-validated time-stamped ledger that chronologically registers all valid transactions.

Block chain and the Internet of Things (IoT) are key technologies that will have a huge impact in the next 10 years for companies in the industrial market. This article describes how these two technologies will improve efficiencies, provide new business opportunities, address regulatory requirements, and improve transparency and visibility.

Block chain is hyped as the silver bullet that might overthrow today’s payment handling. Slowly, the logistics and supply chain management community realizes how profoundly Block chain could affect their industry.

To shed light on this emerging field, we conducted an online survey and asked logistics professionals for their opinion on use case exemplars, barriers, facilitators, and the general prospects of Block chain in logistics and supply chain management.

We found most of our participants are fairly positive about this new technology and the benefits it offers.

However, factors like the hierarchical level, Block chain experiences, and the industry sector have a significant impact on the participants’ evaluation.

We reason that the benefits over existing IT solutions must be carved out more carefully and use cases must be further explored to get a rather conservative industry, like logistics, more excited about Block chain.

II. RELATED WORK

Generally voting is done in polling booths whereas in our system we are doing it in internet as contribution towards the digital India project . Now a days everything is being digitalized moreover people have become lazy so we are using internet for voting . Voting is done by people through voting booth or via post. However, the delay overhead of voting can be prohibitive when numerous participants have to share the post in sequence, making it impractical for time-critical applications . The vote counting had major issues like corruption and slow progress .

We are using various algorithms involved in security such as secure hashing algorithm , elliptical curve digital signature algorithm and data structure concepts like merkle tree for the connectivity of the various data blocks involved in the system.

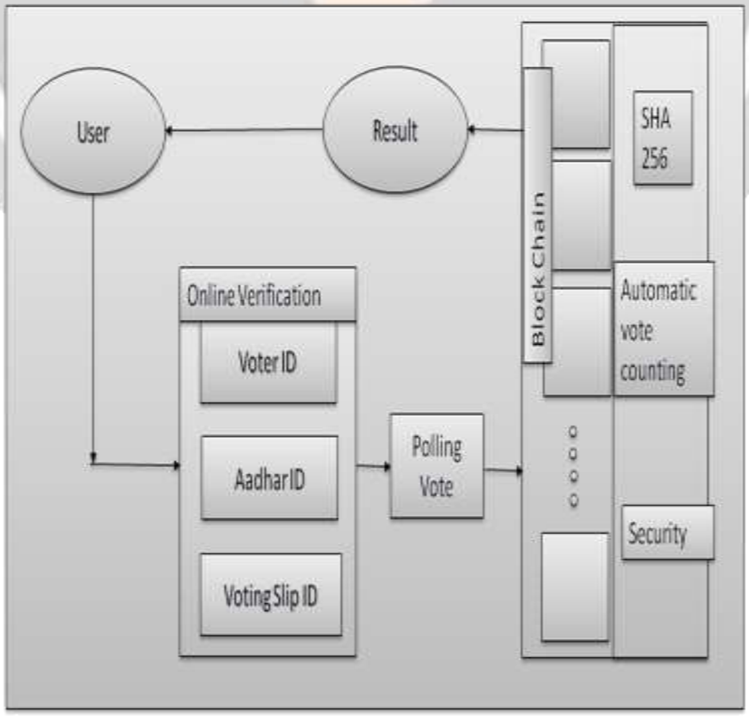
III PROPOSED SYSTEM

We propose a fast and secure Block chain voting scheme called Block chain Voting System BVS, which significantly reduces the delay for collecting and tallying votes. .In BVS, Voters transmit their votes simultaneously by exploiting the blocks in online. Votes are realized by injecting energy to pre-assigned blocks . We show that BVS is secure against hackers and third parties, that attempt to manipulate the voting outcome. Security is achieved by employing cryptography-based authentication and message integrity schemes.

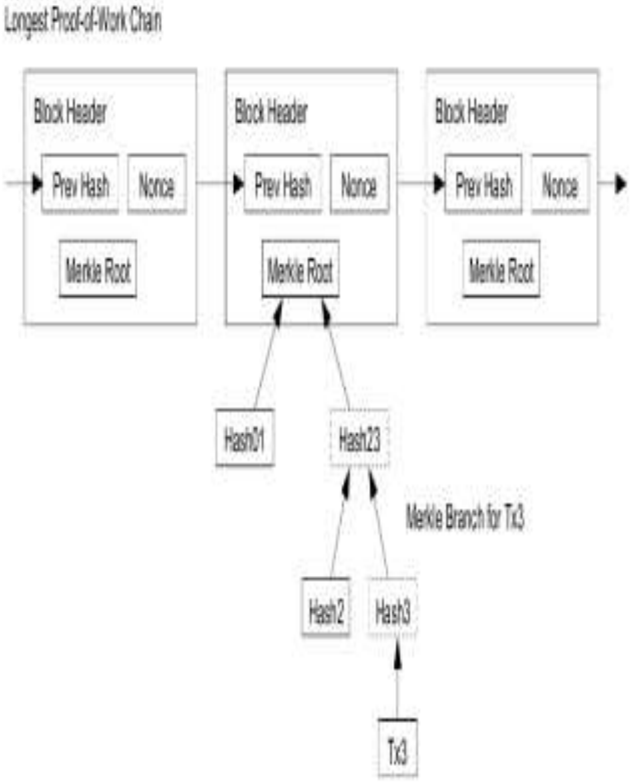
Some advantages of our systems are mentioned below:
1**.**Block chain give more security in decentralised network
2.Result comes within the voting day simultaneously
3.Hacking possibility is very low against the Block chain and cryptography

Ethereum Blocks of chain is an open-source, public, block chain-based distribution of computing platform and operating system featuring smart and contract(scripting) functionality. It supports a modified version of Naka moto consensus via transaction-based state transitions. Ether is one of the crypto currency whose block chain is generated by the Ethereum platform. Ether can be transferred between accounts and used to compensate participant mining nodes for computations performed. Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes.

IV. ARCHITECTURE



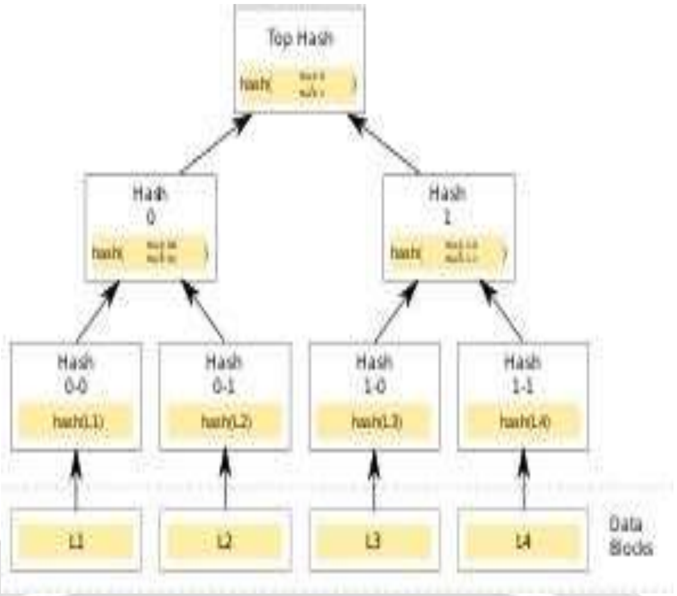
various concepts are being involved in this system architecture as well as may algorithms are being utilised. The System architecture is the conceptual design that defines the structure and behaviour of a system. An architecture description is a formal description of a system organized in a way that supports reasoning about the structural properties of system.



In cryptography and computer science and data structure , a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains. Demonstrating that a leaf node is a part of a given binary hash tree requires computing a number of hashes proportional to the logarithm of the number of leaf nodes of the tree this contrasts with hash lists, where the number is proportional to the number of leaf nodes itself.

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. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with a key aspect of cryptographic hash functions is their collision resistance: nobody should be able to find two different input values that result in the same hash output.

SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4. SHA-2 was published in 2001 by the National Institute of Standards and Technology (NIST) a U.S. federal standard (FIPS).This is the merkle tree data structure algorithm and it involves in connections



The implementation needs to implement the key functionality namely producing a correct message digest for an input string. It is not necessary to mimic all of the calling modes such as adding to a digest one block at a time over subsequent call.

In addition to coding and verifying your implementation, note any challenges your language presented implementing the solution, implementation choices made, or limitations of your solution. Solutions on this page should implement MD5 directly and NOT use built in (MD5) functions, call outs to operating system calls or library routines written in other languages as is common in the original MD5 task.

An original implementation from the specification, reference implementation, or pseudo-code A translation of a correct implementation from another language. A library routine in the same language; however, the source must be included here . The solutions shown here will provide practical illustrations of bit manipulation, unsigned integers, working with little-endian data. Additionally, the task requires an attention to details such as boundary conditions since being out by even 1 bit will produce dramatically different results. Subtle implementation bugs can result in some hashes being correct while others are wrong. Not only is it critical to get the individual sub functions working correctly, even small errors in padding, endian ness, or data layout will result in failure.

Thus using all this algorthims the blocks are created and liked and linking is due to the hash value that is being generated by the various algorithm utilized .

V. CONCLUSION

Security is achieved by employing cryptography-based authentication and message integrity schemes. We propose a fast and secure Block chain voting scheme called Block chain Voting System BVS, which significantly reduces the delay for collecting and tallying votes. The implementation of this concept in reality can reduce the corruption in vote counting and achieve secure result in less time. Our Online-Voting System is secure because user can only vote by entering CNIC. No other information is shown to the user on the polling interface.

On the other hand ADMIN has the only rights to check and count all votes and announce the final result. Although there are many voting apps for this purpose but their security level is not up to that mark .

Voters transmit their votes simultaneously by exploiting the blocks in online. Votes are realized by injecting energy to pre-assigned blocks. The main corruption occurs with the ballot machine by vote changing and false voting or through fake transmission of posts.

The implementation of this concept in reality can reduce the corruption in vote counting and achieve secure result in less time. This would be the best way for voting in the future upcoming days .This would follow the today's digital India's trend and more over many countries are not having a secure voting system and this might be very useful for them too . Even during the last election which took place in united states the people claim that something fraud has take place in the elections. Even in India there were flawless and mistakes in the voting machine , which ever button we press the vote went to the same party . Thus one of the best solution to this problem would be our block chain voting system .

VI. REFERENCES

[1] F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey. Physical Comm., 4(1):40– 62, 2011.

[2] N. Al-Nakhala, R. Riley, and T. Elfouly. Distributed algorithms in wireless sensor networks: an approach for applying binary consensus in a real testbed. Comp. Nets., 2015.

[3] J. G. Andrews, A. Ghosh, and R. Muhamed. Fundamentals of WiMAX: understanding broadband wireless networking. Pearson Education, 2007.

[4] D. Barbara and H. Garcia-Molina. The reliability of voting mechanisms. IEEE Trans. Computers, 36(10):1197–1208, 1987.

[5] W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[6] M. Barborak, A. Dahbura, and M. Malek. The consensus problem in fault-tolerant computing. ACM Comp. Surveys, 25(2):171–220, 1993.

[7] H. Poor, An Introduction to vote Detection and Estimation. New York: Springer-Verlag, 2015.

[8] B. Smith, “An approach to block chain crypto currency (Unpublished work style),” unpublished.

[9] E. H. Miller, “A note on etherum block chain (Periodical style—Accepted for publication),” IEEE Trans. Antennas to be published.

[10] C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 2016.

[11] D. Bharadia, E. McMilin, and S. Katti. Full duplex radios. In Proc. of the SIGCOMM Computer Communication Review, pages 375–386. ACM, 2013.

[12] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava. Integrity codes: Message integrity protection and authentication over insecure channels. Dependable and Secure Computing, IEEE Transactions on, 5(4):208–223, 2008.

[13] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson. Distributed event triggered control for multi-agent systems. IEEE Trans. on Aut. Cntrl., 57(5):1291–1297, 2012.

[14] M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.

[15] J. U. Duncombe, “Voting Device—Part I: An assessment of votes (Periodical style),” *IEEE Trans.* Voting Device, vol. ED-11, pp. 34–39, Jan. 2009.

[16] A. Dutta, D. Saha, D. Grunwald, and D. Sicker. SMACK: a Smart Acknowledgment scheme for broadcast messages in wireless networks. ACM SIGCOMM Comp. Comm. Rev., 39(4):15–26, 2009 .

.