IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN SECURED VOTING SYSTEM USING QR GENERATION

Mrs.R.KIRUTHIKA M.Tech[1], VIJAY.A[2],VAIRAMUTHU.P[3],VIGNESH.A[4]

1ASSISTANT PROFESSER, 2,3,4 UG STUDENTS
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MAHENDRA ENGINEERING COLLEGE, TAMILNADU, INDIA

ABSTRACT

Digital voting has been around for several years now, but it is still slowly being adopted by election bodies around the world. In spite of technology that protects the confidentiality, integrity, and privacy of our data, digital voting systems still raise concerns of election fraud or data leaks. Block chain, the distributed database technology behind Bitcoin, seems like a good fit for digital voting systems, providing a way to keep transactions private, and mechanisms to prevent data alteration. But block chain alone is not enough to address other concerns that come up during elections: how to make sure that the person voting has the right to do so while keeping her identity disconnected from her vote. The user can safely vote from the three level of authentication system OTP, QR code share and Block chain. Here the system contains a secured timestamp and the hash code which is used to identify the fraudulent attacks on the distributed server. We cover these concerns in the following pages, presenting what we believe are suitable solutions for each one. Additionally, it is our opinion that using the methods suggested can work with or without block chain as the storage method. A safe and secured voting is employed using these secured services. The legal and the technology limitations are also analyzed in the block chain distributed ledger.

KEYWORDS: Block chain, Bitcoin, QR code share and Block chain, authentication system OTP.

INTRODUCTION

1.1 NEED FOR THE STUDY

Block chain is a decentralized transaction and data management technology developed first for Bit coin crypto currency. The interest in Block chain technology has been increasing since the idea was coined in 2008. The reason for the interest in Block chain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations. In this research, we have conducted a systematic mapping study with the goal of collecting all relevant research on Block chain technology. Our objective is to understand the current research topics, challenges and future directions regarding Block chain technology from the technical perspective. We have extracted 41 primary papers from scientific databases. The results show that focus in over 80% of the papers is on Bit coin system and less than 20% deals with other Block chain applications including e.g. smart contracts and licensing. The majority of research is focusing on revealing and improving limitations of Block chain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. Many other Block chain scalability related challenges including throughput and latency have been left unstudied. On the basis of this study, recommendations on future research directions are provided for researchers.

1.2 BLOCK CHAIN TRUSTWORTHY

There are three key elements needed to establish trust: 1) identity, or who are who; 2) ownership, or who owns what; and 3) verification, or what's true. Block chains allow users to easily prove their identities, protect ownership of digital assets, and verify transactions without a high-cost intermediary

Who's Who: Block chains solve the identity problem through the use of digital signatures. Each user is given a set of two digital codes (a "private key," similar to an account number, and a "public key," similar to a password) that allows them to easily prove an identity and issue authorized transactions.

Who Owns What: Block chains solve the ownership problem through a technology called "cryptographic hashing." A cryptographic hash is simply a piece of data that has been run through a math function and transformed into a shorter piece of data. In a block chain, each block contains a hashed representation of the data in the previous block. If you change any previous pieces of data, that change will get reflected throughout the chain, making it easy for the system to see and reject fraudulent attempts to manipulate the data. This allows block chains to create "immutable" data, otherwise known as tamper-proof records.

What's True: And, finally, block chains solve the verification problem by making it feasible for a group of people to publicly verify that a transaction is true, without the need for a trusted intermediary. In block chain terminology, this is called "distributed consensus." The ability for block chains to verify transactions with fewer intermediaries is a key benefit that can lead to lower costs for many applications in this report.

1.3 OVERVIEW OF THE PROJECT

As a technology, block chain is quickly becoming unrivaled. Though the internet has long been familiar with other peer-to-peer applications for file sharing, music streaming and more, the idea that these types of networks can provide their own security and resources has only been around since 2008. In the decade since its inception, block chain was mostly tied to the success of the technology that created it, bit coin. Many are finding that block chain's primary value lies in its ability to improve old systems. Enterprising observers saw the technology's potential from the start, as bit coin offered a more secure and transparent payment processing and banking solution than existing ones. In recent years, the same people have used block chain to revolutionize industries far and wide, including cloud storage, smart contracts, crowd funding.

1.4 OBJECTIVES OF THE STUDY

Block chain transaction technology, with all the hype around it, stands to become a further use of an inappropriate and unnecessary technology for voting. Unfortunately, it seems to be touted as the answer to all possible problems, appropriate or not. Just because block chains are the shiny new thing on the Internet is no reason to use them for elections.

Block chains were devised as a way to distribute trust on a network without a central authority. But elections have a central authority the election office which is legally The Authority. The election office does not need a mechanism for distributed trust. In addition, block chains can be very slow, spending a lot of the time verifying that no one is cheating. But verifying that no one is cheating is the responsibility of the election office, and their time and effort would be much better spent verifying that their own central servers are secure and trustworthy, rather than trying to find cheating by unknown bad actors somewhere off on other computers in cyberspace. Internet voting, with or without block chains, does not provide an auditable result or a way for voters to ensure that their votes are counted. The record of the votes is electronic, subject to computer failure, network failure, unintentional mistakes, and deliberate hacks. Computer security is nearly always a game of defense; we ought not to turn democracy over to a process where we can't tell that things have gone wrong until after they have gone wrong.

And finally, one must realize that no single company will invent the entire process on its own. As with all things on the Internet, there are layers upon layers of software, all of which would need to be trusted, and trusted to work together

1.5 LITERATURE REVIEW

[1] Superlight – A Permissionless, Light-client Only Blockchain with Self-Contained Proofs and BLS Signatures

Roman Blum, Thomas Bocek, (2019)

Blockchain protocols are based on a distributed database where stored data is guaranteed to be immutable. The requirement that all nodes have to maintain their own local copy of the database ensures security while consensus mechanisms help deciding which data gets added to the database and keep powerful adversaries from derailing the system. However, since the database that forms the foundation of a blockchain is a continuously growing list of blocks, scalability is an inherent problem of this technology. Some public blockchains require up to terabytes of storage. In this work, we present the concept Superlight with selfcontained proofs, which is designed to improve scalability of a public blockchain, while preserving security and decentralization. Instead of all nodes having a local copy of the whole blockchain to verify a transaction, nodes can derive the validity of a transaction by only using block headers.

[2] Proof-of-Property – A Lightweight and Scalable Blockchain Protocol

Christopher Ehmke, Florian Wessling and Christoph M. Friedrich (2018)

The expansion of blockchain technologies from financial applications to other fields intensifies the problem of an increasing size of data stored in the blockchain. Unfortunately, new participants of the blockchain network are required to download the whole blockchain to gain an overview about the state of the system and to validate incoming transactions. Approaches like IOTA, SegWit or the Lightning Network try to solve the scalability issues of blockchain applications. Unfortunately, they focus on strategies slowing down the blockchain's growth instead of reducing the problems arising from a growing chain or introduce new concepts to oust the linear blockchain altogether. The approach proposed in this paper is based on the idea of Ethereum to keep the state of the system explicitly in the current block but further pursues this by including the relevant part of the current system state in new transactions as well.

SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

The Online Voting system is made for the people of the country residing around the world and wants to vote for their representative. Using Electronic Voting may encompass a range of Internet services from a touch screen kiosk at a polling station to voting online. This Project is developed for the threat free and user oriented Online Voting System. Finger Recognition is a authentication technique. The election can be conducted in two ways the paper ballot election and the automated ballot elections. The automated ballot elections are called the electronic voting. The online voting system is highly developed and the online polling system can be replaced by accurately and directly voting online and immediate results. The online voting system is done by the internet so it can be called the Internet Voting. Fingerprint scanning-essentially provides an identification of a person based on the acquisition and recognition of those unique patterns and ridges in a fingerprint. The actual fingerprint identification process will change slightly between products and systems. The basis of identification, however, is nearly the same. Standard systems are comprised of a sensor for scanning a fingerprint and a processor which stores the fingerprint database and software which compares and matches the fingerprint to the predefined database. Within the database, a fingerprint is usually matched to a reference number, or PIN number which is then matched to a person's name or account. In instances of security the match is generally used to allow or disallow access.

2.2 FEASIBILITY STUDY

Preliminary investigation examine project feasibility, the likelihood the system will be useful to the organization. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging old running system. All system is feasible if they are unlimited resources and infinite time. There are aspects in the feasibility study portion of the preliminary investigation:

- Technical Feasibility
- Operation Feasibility
- Economical Feasibility

2.2.1 Economic Feasibility

A system can be developed technically and that will be used if installed must still be a good investment for the organization. In the economical feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs.

The system is economically feasible. It does not require any addition hardware or software. Since the interface for this system is developed using the existing resources and technologies available at NIC, There is nominal expenditure and economical feasibility for certain.

2.2.2 Operational Feasibility

Proposed projects are beneficial only if they can be turned out into information system. That will meet the organization's operating requirements. Operational feasibility aspects of the project are to be taken as an important part of the project implementation. Some of the important issues raised are to test the operational feasibility of a project includes the following: -

- Is there sufficient support for the management from the users?
- Will the system be used and work properly if it is being developed and implemented?
- Will there be any resistance from the user that will undermine the possible application benefits?

This system is targeted to be in accordance with the above-mentioned issues. Beforehand, the management issues and user requirements have been taken into consideration. So there is no question of resistance from the users that can undermine the possible application benefits.

2.2.3 Technical Feasibility

The technical issue usually raised during the feasibility stage of the investigation includes the following:

- Does the necessary technology exist to do what is suggested?
- Do the proposed equipments have the technical capacity to hold the data required to use the new system?
- Will the proposed system provide adequate response to inquiries, regardless of the number or location of users?
- Can the system be upgraded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access and data security?

Earlier no system existed to cater to the needs of 'Secure Infrastructure Implementation System'. The current system developed is technically feasible. It is a web based user interface for audit workflow at NIC-CSD. Thus it provides an easy access to the users. The database's purpose is to create, establish and maintain a workflow among various entities in order to facilitate all concerned users in their various capacities or roles. Permission to the users would be granted based on the roles specified. Therefore, it provides the technical guarantee of accuracy, reliability and security. The software and hard requirements for the development of this project are not many and are already available in-house at NIC or are available as free as open source. The work for the project is done with the current equipment and existing software technology.

2.4 SOFTWARE DESCRIPTION

FEATURES OF SOFTWARE

JAVA SERVER PAGE (JSP)

Java Server Page (JSP) is a technology for controlling the content or appearance of Web pages through the use of servlets, small programs that are specified in the Web page and run on the Web server to modify the Web page before it is sent to the user who requested it. Sun Microsystems, the developer of Java, also refers to the JSP technology as the Servlet application program interface (API). JSP is comparable to Microsoft's Active Server Page (ASP) technology. Whereas a Java Server Page calls a Java program that is executed by

the Web server, an Active Server Page contains a script that is interpreted by a script interpreter (such as VBScript or JScript) before the page is sent to the user. Architecturally, JSP may be viewed as a high-level abstraction of Java servlets. JSPs are translated into servlets at runtime, therefore JSP is a Servlets; each JSP servlet is cached and re-used until the original JSP is modified.JSP can be used independently or as the view component of a server-side model–view–controller design, normally with JavaBeans as the model and Java servlets (or a framework such as Apache Struts) as the controller. This is a type of Model 2 architecture.

JSP allows Java code and certain pre-defined actions to be interleaved with static web markup content, such as HTML, with the resulting page being compiled and executed on the server to deliver a document. The compiled pages, as well as any dependent Java libraries, contain Java byte code rather than machine code. Like any other Java program, they must be executed within a Java virtual machine (JVM) that interacts with the server's host operating system to provide an abstract, platform-neutral environment. JSPs are usually used to deliver HTML and XML documents, but through the use of OutputStream, they can deliver other types of data as well. The Web container creates JSP implicit objects like request, response, session, application, config, page, pageContext, out and exception. JSP Engine creates these objects during translation phase.

SYNTAX

JSP pages use several delimiters for scripting functions. The most basic is <% ... %>, which encloses a JSP scriptlet. A scriptlet is a fragment of Java code that is run when the user requests the page. Other common delimiters include <%= ... %> for expressions, where the scriptlet and delimiters are replaced with the result of evaluating the expression, and directives, denoted with <%@ ... %>.Java code is not required to be complete or self-contained within a single scriptlet block. It can straddle markup content, provided that the page as a whole is syntactically correct. For example, any Java if/for/while blocks opened in one scriptlet must be correctly closed in a later scriptlet for the page to successfully compile. Content which falls inside a split block of Java code (spanning multiple scriptlets) is subject to that code. Content inside an if block will only appear in the output when the if condition evaluates to true. Likewise, content inside a loop construct may appear multiple times in the output, depending upon how many times the loop body runs.

COMPILER

A Java Server Pages compiler is a program that parses JSPs, and transforms them into executable Java Servlets. A program of this type is usually embedded into the application server and run automatically the first time a JSP is accessed, but pages may also be precompiled for better performance, or compiled as a part of the build process to test for errors. Some JSP containers support configuring how often the container checks JSP files timestamps to see whether the page has changed. Typically, this timestamp would be set to a short interval (perhaps seconds) during software development, and a longer interval (perhaps minutes, or even never) for a deployed Web application.

BACK END (MYSQL)

MySQL is the world's most used open source relational database management system (RDBMS) as of 2008 that run as a server providing multi-user access to a number of databases. The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation.

MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack—LAMP is an acronym for "Linux, Apache, MySQL, Perl/PHP/Python." Free-software-open source projects that require a full-featured database management system often use MySQL.

For commercial use, several paid editions are available, and offer additional functionality. Applications which use MySQL databases include: TYPO3, Joomla, Word Press, phpBB, MyBB, Drupal and other software built on the LAMP software stack. MySQL is also used in many high-profile, large-scale World Wide Web products, including Wikipedia, Google (though not for searches), ImagebookTwitter, Flickr, Nokia.com, and YouTube.

Graphical

The official MySQL Workbench is a free integrated environment developed by MySQL AB, which enables users to graphically administer MySQL databases and visually design database structures. MySQL Workbench replaces the previous package of software, MySQL GUI Tools. Similar to other third-party packages, but still considered the authoritative MySQL frontend, MySQL Workbench lets users manage database design & modeling, SQL development (replacing MySQL Query Browser) and Database administration (replacing MySQL Administrator).MySQL Workbench is available in two editions, the regular free and open source Community Edition which may be downloaded from the MySQL website, and the proprietary Standard Edition which extends and improves the feature set of the Community Edition.

Command line

MySQL ships with some command line tools. Third-parties have also developed tools to manage a MySQL server, some listed below. Maatkit - a cross-platform toolkit for MySQL, PostgreSQL and Memcached, developed in Perl Maatkit can be used to prove replication is working correctly, fix corrupted data, automate repetitive tasks, and speed up servers. Maatkit is included with several GNU/Linux distributions such as CentOS and Debian and packages are available for Programming. MySQL works on many different system platforms, including AIX, BSDi, FreeBSD, HP-UX, eComStation, i5/OS, IRIX, Linux, Mac OS X, Microsoft Windows, NetBSD, Novell NetWare, OpenBSD, OpenSolaris, OS/2 Warp, QNX, Solaris, Symbian, SunOS, SCO Open Server, SCO UnixWare, Sanos and Tru64. A port of MySQL to OpenVMS also exists.

MySQL is written in C and C++. Its SQL parser is written in yacc, and a home-brewed lexical analyzer. Many programming languages with language-specific APIs include libraries for accessing MySQL databases. These include MySQL Connector/Net for integration with Microsoft's Visual Studio (languages such as C# and VB are most commonly used) and the JDBC driver for Java. In addition, an ODBC interimage called MyODBC allows additional programming languages that support the ODBC inter image to communicate with a MySQL database, such as ASP or ColdFusion. The HTSQL - URL-based query method also ships with a MySQL adapter, allowing direct interaction between a MySQL database and any web client via structured URLs.

Features

As of April 2009, MySQL offered MySQL 5.1 in two different variants: the open source MySQL Community Server and the commercial Enterprise Server. MySQL 5.5 is offered under the same licenses. They have a common code base and include the following features:

- A broad subset of ANSI SQL 99, as well as extensions
- Cross-platform support
- Stored procedures
- Triggers
- Cursors
- Updatable Views
- Information schema
- Strict mode (ensures MySQL does not truncate or otherwise modify data to conform to an underlying data type, when an incompatible value is inserted into that type)
- X/Open XAdistributed transaction processing (DTP) support; two phase commit as part of this, using Oracle's InnoDB engine
- Transactions with the InnoDB, and Cluster storage engines
- SSL support
- Query caching
- Sub-SELECTs (i.e. nested SELECTs)
- Replication support (i.e. Master-Master Replication & Master-Slave Replication) with one master per slave, many slaves per master, no automatic support for multiple masters per slave.
- Full-text indexing and searching using MyISAM engine
- Embedded database library

- Partititoned tables with pruning of partitions in optimiser
- Shared-nothing clustering through MySQL Cluster
- Hot backup (via mysqlhotcopy) under certain conditions
- Multiple storage engines, allowing one to choose the one that is most effective for each table in the application (in MySQL 5.0, storage engines must be compiled in; in MySQL 5.1, storage engines can be dynamically loaded at run time): Native storage engines (MyISAM, Falcon, Merge, Memory (heap), Federated, Archive, CSV, Blackhole, Cluster, EXAMPLE, Maria, and InnoDB, which was made the default as of 5.5). Partner-developed storage engines (solidDB, NitroEDB, ScaleDB, TokuDB, Infobright (formerly Brighthouse), Kickfire, XtraDB, IBM DB2). InnoDB used to be a partner-developed storage engine, but with recent acquisitions, Oracle now owns both MySQL core and InnoDB.

3.1 PROPOSED SYSTEM

Building electronic voting systems and identifies the legal and technological limitations of using block chain as a service for realizing such systems. The paper starts by evaluating some of the popular block chain frameworks that offer block chain as a service. We then propose a novel electronic voting system based on block chain that addresses all limitations we discovered. More generally this paper evaluates the potential of distributed ledger technologies through the description of a case study, namely the process of an election and implementing a block chain-based application which improves the security and decreases the cost of hosting a nationwide election. The block chain structure is an append-only data structure, such that new blocks of data can be written to it, but cannot be altered or deleted the blocks are chained in such a way that each block has a hash that is a function of the previous block, providing the assurance of immutability. Three level of security is been implemented with the added technology. User and the candidate can get the OTP and the QR code for the secured voting session. In our proposal, we will use a permission block chain, a variation of the consortium-based chains, which uses the proof-of-authority (POA) consensus algorithm. In proof-of authority-based networks, transactions and blocks are validated by approved accounts, known as validates. This process is automated and does not require that validates to be constantly monitoring their computers.

3.2 MODULES

- Registration
- OTP authentication
- Login
- QR share
- Block Chain Voting
- Intimation

MODULE DESCRIPTION

Registration

The register module provides a conceptual framework for entering data on those user and the candidate in a way that: eases data entry & accuracy by matching the MySQL database entry to the data source (usually paper files created at point of care), ties easily back to individual user and the candidate records to connect registers to the user details and the candidate details. It collects data elements to enable better handling for the voter's data and the candidate data. The data will be stored in the block chain based storage system. A block chain-based storage system prepares data for storage by creating data shards or segments, encrypting the shards, generating a unique hash for each shard and creating redundant copies of each shard. The replicated shards are then distributed across the decentralized nodes in the block chain infrastructure. Block chains are stored in computers within the system, also named as nodes.

Block Chain Voting

The blockchain system is the system on which the actual voting takes place. The users' vote is sent to the one of the nodes on the system depending on the load on each node. The node then adds the transaction to the blockchain depending on the smart contracts that exist on each node. The smart contracts are the rules that the nodes follow to not only verify but also add the vote in the system. Each node follows the smart contract to verify the vote. The blockchain is a private system and is not accessible to the public directly. The system will currently have node server in each state to ensure a distributed network traffic on the system. The process of voting has two steps in the old process, i.e. registering to vote and the process of voting itself. The proposed

system will have an extra step, i.e. the ability for the user to verify their vote. This is an important step where the user can get a confirmation of their vote. The other steps include counting the votes by the organizer and recounting in case of any discrepancies. The process of registering to vote begins with the user interacting with the Authentication Server via a website. The AS contains information about voters in a database. The user enters his/her Personally Identifiable Information (PII) and scans supporting documentation to upload into the system along with an email address. The users' picture is also taken for verification. If the information is verified and is correct, the user is allowed to create an account. The user enters a username of their choice and a password to log in. This information is stored separately and not linked to the users' PII. This ensures privacy and anonymity while voting. Also an entry is made next to the users' database entry storing whether he/she has registered to vote. If the users' information cannot be verified, he/she is not allowed to create an account.

Intimation

The block chain server are connected with the inter server systems where the vote count are got stored in each block or node. The data change in any block will be mentioned with the time stamp and they can be intimated to the admin. The main process here is that the total count cannot be taken since the change in the data will also change the hash code of the server. If the server hash code get changes then the data cannot be connected together to gather the total count of the vote. If the changes of the value will be notified as "data modified".

SYSTEM IMPLEMENTATION

The block chain technology was introduced in 2008 when Satoshi Nakamoto created the first crypto currency called Bit coin. The Bit coin block chain technology uses a decentralized public ledger combined with PoW(Proof-of-Work) based stochastic consensus protocol, with financial incentives to record a totally ordered sequence of blocks, the block chain. The chain is replicated, cryptographically signed and publicly verifiable at every transaction so that no-one can tamper with the data that has been written onto the block chain. The block chain structure is an append-only data structure, such that new blocks of data can be written to it, but cannot be altered or deleted The blocks are chained in such a way that each block has a hash that is a function of the previous block, providing the assurance of immutability. Whereas the block chain publishes all elements of the entire chain, in general other types of block chain can be public, private or consortium based. Public block chains grant access to read and ability to create a transaction to any user on that network. The block chain based system will add the process by which the user can vote with the secured system.

The login can be verified and check with multiple users where the user will get an authentication for every login session where the unknown user cannot able to use the system for the voting system. The change in the block server can be intimated and the result is verified with the execution.

6.1 CONCLUSION

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this paper, we introduced a unique, block chain-based electronic voting system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system

6.2 FUTURE ENHANCEMENT

In future system the flaws of the developed project can be enhanced. Blockchain-based voting, which relies on a decentralized, distributed digital ledger is vulnerable to many of the security flaws inherent in internet voting, such as the potential for malware to alter votes on a voter's local device before the ballot is transmitted and the lack of secret ballots.

REFERENCES

[1] Aishwarya Shete, Atul Lahade, Tejas Patil, Prof. Renuka Pawar, DHCP Protocol using OTP Based Two-Factor Authentication, d International Conference on Trends in Electronics and Informatics, 201

[2] Ashish Singh, Kakali Chatterjee, SecEVS : Secure Electronic Voting System Using Blockchain Technology, International Conference on Computing, Power and Communication Technologies, pp:863- 867, 2018

[3] Axel Schmidt, Lucie Langer, Johannes Buchmann, Specification of a Voting Service Provider, First International Workshop on Requirements Engineering for E-Voting System, 2009

[4] Christopher Ehmke, Florian Wessling, Christoph M. Friedrich, Proof-of-Property – A Lightweight and Scalable Blockchain Protocol, International Workshop on Emerging Trends in Software Engineering for Blockchain, 2018

[5] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, Blockchain-Based E-Voting System International Conference on Cloud Computing, pp: 983-986, vol:11, 2018

[6] Jordi Cucurull , Sandra Guasch , Alex Escala , Guillermo Navarro-Arribas and V´ıctor Ac, QR Steganography A Threat to New Generation Electronic Voting Systems, pp: 978-989, vol:75, 2014

[7] Pei-Yu Lin, Distributed Secret Sharing Approach with Cheater Prevention based on QR Code, IEEE Transactions on Industrial Informatics, 2015

[8] Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur Rahman, Biometrically Secured Electronic Voting Machine, IEEE Region 10 Humanitarian Technology Conference, 2017

[9] Roman Blum, Thomas Bocek, Superlight – A Permissionless, Light-client Only Blockchain with Self-Contained Proofs and BLS Signatures, 2019

[10] Tara Salman, Raj Jain, Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making, pp: 457-465, vol: 4, 2017