ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Prevent election data tampering using block chain technology

Ms. P. Vanitha[1], S. Aswin[2], R. Aswin[2], Indra Kumar, B[2], Jaya Suriya[2]

[1]Assistant Professor, [2]UG Students

ABSTRACT

Despite the claimed benefits of e-voting initiatives, wider adoption of e-voting mechanisms and implementation processes is slower than expected. Several technical, social, and cultural challenges hinder generality and applicability of e-voting. Amongst them, the evaluation and harmonization of e-voting systems, given different legal and statutory frameworks, is still an important challenge to overcome. Yet, only a few works have addressed this topic in the field. Block chain is considered one of the best data securing technology which is widely used in bit coin and crypto currency. Block Chain can be implemented in voting machines to avoid vote tampering.General Terms Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, and Algorithms etc..,

Keywords: E-Voting, Block Chain, IOT.

INTRODUCTION

Electronic voting is voting that uses electronic means to either aid or take care of casting and counting votes. Depending on the particular implementation, e-voting may use standalone electronic voting machines or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results. A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal successfully with strong requirements with security, accuracy, integrity, privacy, auditability, accessibility etc.

A block chain is, in the simplest of terms, a time-stamped series of immutable record of data that is managed by cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) are secured and bound to each other using crypto graphic principles.

In this paper, we use two technologies, IoT and Block Chain. These will give us much secure and better voting technology which can be effectively used to solve the problems like Vote tampering.

A block chain carries no transaction cost. (An infrastructure cost yes, but no transaction cost.) The block chain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. The verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history. Falsifying a single record would mean falsifying the entire chain in millions of instances. That is virtually impossible. Bitcoin uses this model for monetary transactions, but it can be deployed in many other ways.Information held on a block chain exists as a shared and continually reconciled database. This is a way of using the network that

Author for correspondence:
Department of Computer Science Engineering.

has obvious benefits. The block chain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

The block chain can be described as an immutable, cumulative ledger, with consensus protocol working to maintain this ledger of all valid transactions on every node in the network. Block chain technology originates from the underlying architectural design of the crypto currency bitcoin. It is a form of distributed database where records take the form of transactions, a block is a collection of these transactions. With the use of block chains a secure and robust system for digital voting can be devised.

LITERATURE SURVEY

The main idea in a liquid democracy [6] is that the voter has the power, at any given moment, to review the way his vote was cast in terms of a specific legislative proposal or a bill.

This allows people with domain-specific knowledge to better influence the outcome of decisions, which should lead to an overall better governance. The concept of liquid democracy be a possible answer to the public requests, but there are technical and social barriers in the way. The solution to the technical concerns associated with the liquid democracy concept could be vital for the evolution of democracy as we know it. [1]

Below, we list our envisioned essential requirements that need to be fulfilled by an e-voting system in order for it to effectively be used in a national election:

- An election system should not enable coerced voting.
- An election system should not enable traceability of a vote to a voters identifying credentials.
- An election system should ensure and proof to a voter, that the voters vote, was counted, and counted correctly.
- An election system should not enable control to a third party to tamper with any vote.
- An election system should not enable a single entity, Control over tallying votes and determining an elections result.
- An election system should only allow eligible individuals to vote in an election

In our proposal, we will use a permissioned 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 validators.[3] This process is automated and does not require the validators to be constantly monitoring their computers. A permissioned block chain which uses the POA consensus algorithm enables us to set Restrictions on a set of selected known entities to validate and certify transactions on the block chain and censor transaction arbitrarily, with their identity and reputation at stake. This other wise needs to be done by miners on a public block chain which uses the proof-of-work consensus algorithm. Rather than employing mining fees, like the public block chains in operation require, using a permissioned block chain, validators get paid for the service they provide by acting as validator sin the system.

PROPOSED SYSTEM

The block chain can be described as an immutable, cumulative ledger, with consensus protocol working to maintain this ledger of all valid transactions on every node in the network. 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 transactions; a block is a collection of these transactions [5]. With the use of block chains a secure and robust system for digital voting can be devised.In our work, each election process is represented by a set of smart contracts, which are instantiated the block chain by the election administrators. The main advantages are Highly Secure, prevents all sort of misusage and gives proper user interface. 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. [2]

The protocol proposed was focused on the first class, where strong voter privacy was the primary objective which had two challenges. First challenge was that there exists no trusted third party. With a trusted third party, many security problems can be easily solved, but could lead to the 'trusted' third party to become the one who breaks the security policy. The goal therefore was to eliminate the use of a trusted third party altogether. The second challenge was that there would be no voter-to-voter private channels to ensure dispute freeness, I e everybody could check whether all voters had followed the protocol faithfully.

E-voting systems will be beneficial to all people who are involved in elections. For example, administrators can improve operation of tasks for elections, and voters can vote in an election anytime and anywhere. In addition, ideal e-voting systems have transparency, completeness (only voters have the right to vote and their votes are correctly counted), and verifiability (voters can check that their vote is correctly counted), and therefore a better solution is required

METHODOLOGY

In order to perform authenticated voting system our system is proposed to use electronic id to identify the voter. The machine is connected to a database via IoT and all the voting is implemented through Block Chain.

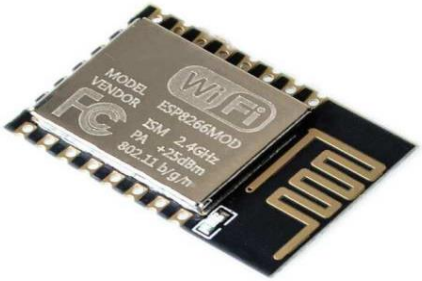
ESP8266-12E

Description

The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability.

The chip first came to the attention of western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer Ai-Thinker. This small module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands. However, at first there was almost no English-language documentation on the chip and the commands it accepted. The very low price and the fact that there were very few external components on the module, which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, chip, and the software on it, as well as to translate the Chinese documentation.

The ESP8285 is an ESP8266 with 1 MiB of built-in flash, allowing for single-chip devices capable of connecting to Wi-Fi.



Arduino IDE

Description

He Arduino integrated development environment is a cross-platform application that is written in the programming language Java. It is used to write and upload programs to Adriano board.

The source code for the IDE is released under the GNU General Public License, version 2The Adriano IDE supports the languages C and C++ using special rules of code structuring. The Adriano IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub main() into an executable cyclic executive program with the GNU tool chain, also included with the IDE distribution. The Adriano IDE employs the program argued to convert the executable code into a text file in hexadecimal encoding that is loaded into the Adriano board by a loader program in the board's firmware.

Inbuilt ICSP Programmer

Description

In-system programming (ISP), also called **in-circuit serial programming** (ICSP), is the ability of some programmable logic devices, microcontrollers, and other embedded devices to be programmed while installed in a complete system, rather than requiring the chip to be programmed prior to installing it into the system. There are several mutually-incompatible in-system semi crocontroller devices, including PIC microcontrollers, AVRs, and the Parallax Propeller. ICSP has been primarily implemented by Microchip Technology for programming PIC and dsPIC devices. Typically, chips supporting ISP have internal circuitry to generate any necessary programming voltage from the system's normal supply voltage, and communicate with the programmer via a serial protocol. Most programmable logic devices use a variant of the JTAG protocol for ISP, in order to facilitate easier integration with automated testing procedures. Other devices usually use proprietary protocols or protocols defined by older standards. In systems complex enough to require moderately large glue logic, designers may implement a JTAG-controlled programming subsystem for non-JTAG devices such as flash memory and microcontrollers, allowing the entire programming and test procedure to be accomplished under the control of a single protocol.

FIGURES

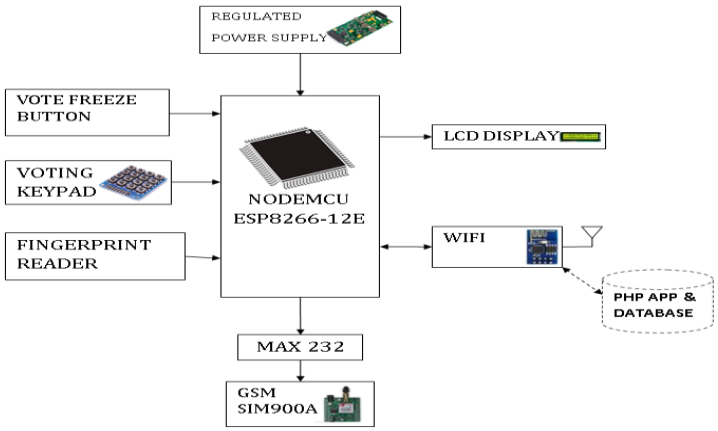


Fig 1: Block Diagram

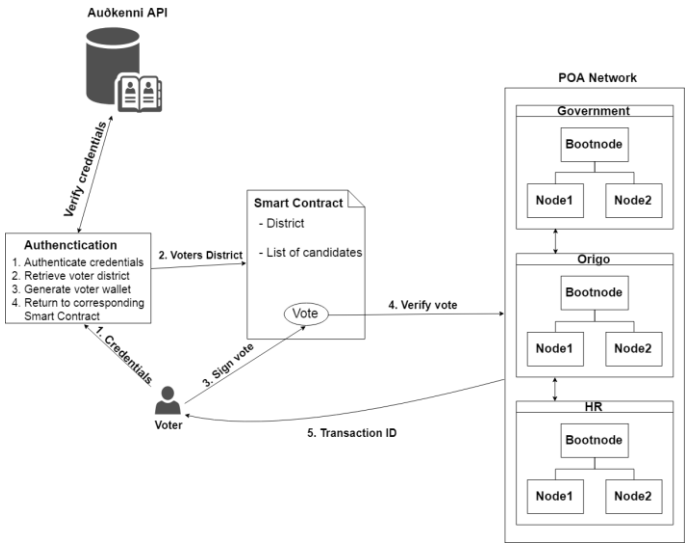


Fig 2: Voter authenticates himself and casts vote

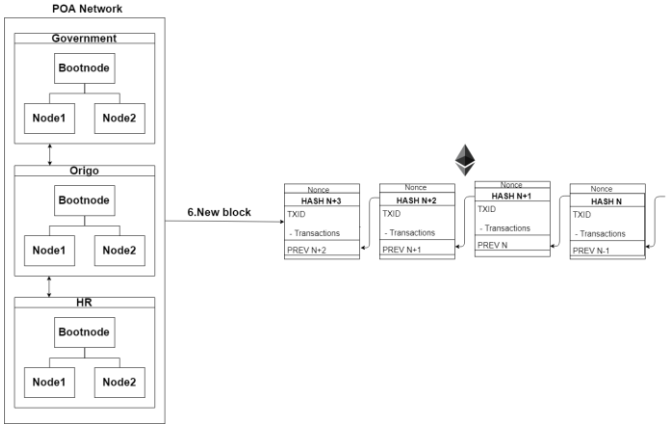


Fig 3: Block added to the block chain

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. By comparison to previous work, we have shown that the block chain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the today's scheme and offer new possibilities of transparency.

REFERENCES

[1]. D. Springall et al., "Security Analysis of the Estonian Internet Voting System," Proc. 21st ACM Conf. Comput. Commun. Secur., no. 2014, 12.

[2]. TechCrunch. 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/ 2018.

[3]. Vitalik Buterin. Ethereum White Paper. Available at: https:// github.com/ ethereum/ wiki/ wiki/ White-Paper. 2015

[4]. X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," Adv. Cryptol. – EUROCRYPT, pp. 19–35, 2005. PANIZO ET AL.: E-VOTING SYSTEM EVALUATION BASED ON THE COUNCIL OF EUROPE RECOMMENDATIONS: HELIOS VOTING 11, 2005.

[5]. Manuel Blum, Alfredo De Santis, Silvio Micali and Giuseppe Persiano. Non-Interactive Zero-Knowledge Available at: https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Zero\%20Knowledge/Noninteractive_Zero-Knowkedge.pdf 1988

[6]. Amot Fiat and Adi Shamir. (1986). How to Prove Yourself: Available at: https://www.math.uni-frankfurt.de/~dmst/teaching/SS2012/Vorlesung/ Fiat.Shamir.pdf

[7]. Alin Tomescu and Srinivas Devadas. Catena: Efficient Nonequivocation via Bitcoin Available at: https://people.csail.mit.edu/ alinush/papers/catena-sp2017.pdf 2017.

[8]. Jelurida, "Jelurida". Available at: 2017 https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf

[9]. Manuel Blum, Alfredo De Santis, Silvio Micali and GiuseppePersiano. Non-Interactive Zero-Knowledge Available at: https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers 1988.

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

[11]. Patrick McCorry, Siamak F. Shahandashti and Feng Hao. ASmart Contract for Boardroom Voting with Maximum Voter PrivacyAvailable at: https://eprint.iacr.org/2017/110.pdf 2017.

[12]. Feng Hao, P.Y.A. Ryan and Piotr Zielinski. Anonymous voting by two-round public discussion. Available at: http://homepages.cs.ncl.ac.uk/feng.hao/files/OpenVote_IET.pdf 2008.

[13]. Nca.tandfonline.com. Pirates on the Liquid Shores ofLiberal Democracy: Movement Frames of European Pirate Parties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/13183222.2015.1017264#.Wr0zCnVl8YR 2015.

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

[15]. Mihir Bellare & Phillip Rogaway. Random Oracles are Practical: 1995. A Paradigm for Designing Efficient Protocols Availablehttps:/cseweb.ucsd.edu/~mihir/papers/ro.pdf