International Journal of Computer Techniques -– Volume 8 Issue 2, March 2021

RESEARCH ARTICLE OPEN ACCESS

Digital Voting System Using Blockchain Technology

S.Sambasivam MCA., M.Phil.*, M.Sowndhar**

* Professor, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: sammy2173@gmail.com

** Final MCA, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: sowndharmani444@gmail.com

****

ABSTRACT

Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a completely unique electronic system supported blockchain that addresses a number of the restrictions in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. In particular, we evaluate the potential of distributed ledger technologies through the outline of a case study; namely, the process of an election, and therefore the implementation of a blockchain based application, which improves the security and decreases the cost of hosting a nationwide election

Keywords — **Blockchain technology, Hash key Algorithm.**

****

I. INTRODUCTION

Electronic voting systems are the topic of active research for decades, with the goal to minimize the cost of running an election, while ensuring the election integrity by fulfilling the security, privacy and compliance requirements[1]. Replacing the normal pen and paper scheme with a replacement election system has the potential to limit fraud while making the voting process traceable and verifiable [2].

Blockchain is a distributed, immutable, incontrovertible, public ledger This new technology has three main features:

(i) Immutability: Any proposed “new block” to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the blockchain gets its name from, and prevent tampering with the integrity of the previous entries.

(ii) Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability(by eliminating one point of failure)and provides third-party verifiability as all nodes maintain the consensus version of the ledger.

(iii) Distributed Consensus: A distributed consensus protocol to determine who can append he next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.

These features are in part achieved through advanced cryptography, providing a security level greater than any previously known record-keeping system. Blockchain technology is therefore considered by many [3], including us, to have a substantial potential as a tool for implementing a replacement modern voting process.

This paper evaluates the use of blockchain as a service to implement an electronic voting (e-voting)system. The paper makes the following original contributions:(i)propose a blockchain based e-voting system that uses “permissioned blockchain”, and (ii) review of existing blockchain frameworks suited for constructing blockchain-based e-voting system.

II. PRELIMINARIES OF E-VOTING AND BLOCKCHAIN

In this section, we first elaborate on the planning considerations when constructing an electronic voting system. Then, we provide an summary of blockchain and smart contract technology and its respective feasibility as a service for implementing an e-voting system.

A. Design considerations

After evaluating both existing e-voting systems and therefore the requirements for such systems to be effectively utilized in a national election, we constructed the subsequent list of requirements for a viable e-voting system:

(i) An election system should not enable coerced voting.
(ii) An election system should allow a way of secure authentication via an identity verification service.
(iii) An election system shouldn't allow traceability from votes to respective voters.
(iv) An election system should provide transparency, in the form of a verify able assurance to every voter that their vote was counted, correctly, and without risking the voter’s privacy.
(v) An election system should prevent any third party from tampering with any vote.
(vi) An election system shouldn't afford any single entity control over tallying votes and determining the results of an election.
(vii) An election system should only allow eligible individuals to vote in an election.

B. Blockchain as a service

The blockchain is an append-only data structure, where data is stored during a distributed ledger that can't be tampered with or deleted. This makes the ledger immutable. The blocks are chained in such how that every block features a hash that's a function of the previous block, and thus by induction the complete prior chain, thereby providing assurance of immutability. There are two differing types of blockchains, with different levels of restrictions supported who can read and write blocks.

A public blockchain is readable and writeable for everybody in the world. This type is popular for cryptocurrencies. A private blockchain sets restrictions on who can read or interact with the blockchain. Private blockchains are also known as being permissioned, where access can be granted to specific nodes that may interact with the blockchain [4]. In addition to cryptocurrency, blockchain provides a platform for building distributed and immutable applications or smart contracts.

Smart contracts are programmable contracts that automatically execute when pre-defined conditions are met. Similar to conventional written contracts, smart contracts are used as a legally binding agreement between parties. Smart contracts automate transactions and allow parties to reach agreements directly and automatically, without the necessity for a middleman. Key benefits of smart contracts compared to conventional written contracts are cost saving, enhanced efficiency and risk reduction. Smart contracts redefine trust, as contracts are visible to all or any the users of the blockchain and may, therefore, be easily verified. In this work, we define our e-voting system based on smart contracts [5].

C. BLOCKCHAIN AS A SERVICE FOR E-VOTING

This section proposes a replacement e-voting system supported the identified voting requirements and block chain as a service. We explain the setup of the blockchain, define the smart contract for e-voting which will be deployed on the blockchain and show how the proposed system satisfies the envisioned voting requirements.

A. Blockchain setup

In order to satisfy the privacy and security requirements for e-voting, and to make sure that the election system shouldn't enable coerced voting, voters will need to choose a supervised environment. In our work, we setup a Go Ethereum [7][9] permissioned Proof-of Authority (POA) blockchain to achieve these goals. POA uses an algorithm that delivers comparatively fast transactions through a consensus mechanism based on identity as a stake. The reason for using Go-Ethereum for the blockchain infrastructure is explained in sub-section C. The structure of the blockchain is illustrated in Figure 1 and mainly consists of two types of nodes.

(i) **District node:** Represent each voting district. Each district node has a software agent that autonomously interacts with the "bootnode" and manages the life cycle of the smart contract on that node. When the election administrator (see smart contract section) creates an election, a ballot smart contract is distributed and deployed onto its corresponding district node. When the ballot smart contracts are created, each of the corresponding district nodes is given permission to interact with their corresponding contract. When an individual voter casts her vote from her corresponding smart contract, the vote data is verified by the majority of the corresponding district nodes and each vote they agree on is appended onto the blockchain.

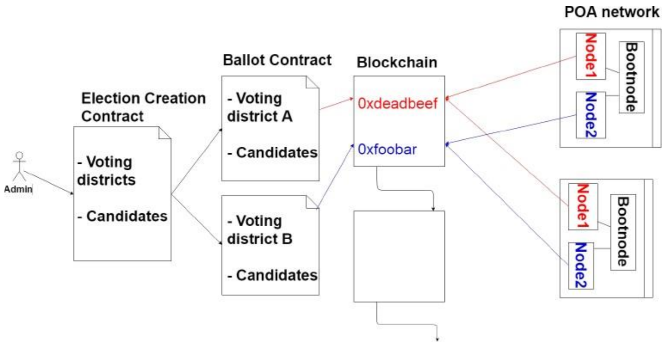

Fig. 1: Election as a smart contract

(ii) **Bootnode:** Each institution, with permissioned access to the network, host a boot node. A bootnode is a discovery and coordination service that helps the district nodes to discover each other and communicate. The bootnode does not keep any state of the blockchain and is run on a static IP in order that district nodes find their peers faster [6]

After fixing a secure and personal blockchain, the next step is to define and deploy a sensible contract that represents the e-voting process on the blockchain infrastructure.

B. Election as a smart contract

Defining a smart contract includes three parts: (1)identifying the roles that are involved within the agreement (the election agreement in our case), (2) the agreement process (i.e., election process), and (3) the transactions (i.e., voting transaction)used in the smart contract.

1) Election roles: The roles during a smart contract include the parties need to participate in the agreement. The election process has the following roles:

(i) Election administrator: To manage the lifecycle of an election. Multiple trusted institutions and companies may be enrolled in this role. The election administrators create the election, register voters, decide the lifetime of the election and assign permissioned nodes.

(ii) Voter: a private who is eligible to vote. Voters can authenticate themselves load election ballots, cast their vote and verify their vote after an election is over.

2) Election process: In our work, each election process is represented, by a group of smart contracts, which are deployed on the blockchain by the election administrators as shown in Figure1. A smart contract is defined for every of the voting districts. The subsequent are the most activities within the election process:

(i) Election creation: Election administrators create election ballots employing a smart accept which the administrator defines a list of candidates for each voting district. The smart contracts are then written onto the blockchain, where district nodes gain access to interact with their corresponding smart contract.

(ii) Voter registration: The registration of voters phase is conducted by the election administrators. When an election is created the election administrators must define a deterministic list of eligible voters. This might require a component for a government identity verification service to securely authenticate and authorize eligible individuals. Using such a service is necessary to satisfy the requirement of secure authentication as this is not guaranteed.

TABLE I: Example of an transaction in our system

TxHash	Block	To	Value
0xdeadbeef…	1337	N1SC	D
0xG1345edf…	1330	N2SC	P

.

(iii) Tallying results: The tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for his or her corresponding location in its own storage.

(iv) erifying votes within the voting transaction, each voter receives the transaction ID of his vote. In our e-voting system, voters can use this transaction ID and attend an official election site (or authority)using a blockchain explorer and (after authenticating themselves using their electronic identification) locate the transaction with the corresponding transaction ID on the blockchain. Voters can, therefore, see their votes on the blockchain, and verify that the votes were listed and counted correctly. This type of verification satisfies the transparency requirements while they preventing traceability of votes.

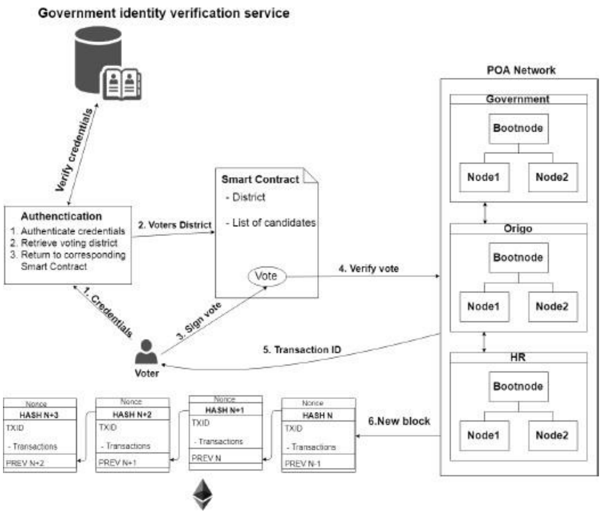

Fig. 2: The voting process

3) Voting transaction Each voter interacts with a ballotsmart contract for her corresponding voting district. This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain. Each individual voter receives the transaction ID for his or her vote for verification purposes. Every vote that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction then appended on the blockchain. Figure 2 is a visual representation of this process. A

transaction in our proposed system (see Table I) has information on i) the transaction ID, ii) the block which the transaction isfound at, iii) to which smart contract the transaction was sent - which
indicates from which voting district the vote was cast, and iv) the value of the transaction, i.e. the vote, indicating which entity (party) the voter voted for. A voting transaction in our system, therefore, reveals no information about the individual voter who cast any particular vote.

B. Evaluating blockchain implementations

As explained at the beginning of this section, in order to satisfy the privacy, security and transparency requirements for e-voting and to make sure that the election system shouldn't enable coerced voting, in our work, we are using a private(permissioned) blockchain for setting up our blockchain infrastructure, where the smart contracts are deployed. In this subsection, we consider three blockchain frameworks (See Table II) for implementing and then deploying our election smart contracts. Those are Exonum, Quorum and Geth.

Exonum: The Exonum blockchain is robust end-to-end with its full implementation done with the programming language Rust. Exonum is built for private blockchains. It has a customizedByzantine algorithm that won't to achieve consensus in the network. Exonum can support up to 5000 transactions per second. Unfortunately, a limitation of the framework is that Rust is the only programming language in the current version, which limits the Developers to the constructs available in that language. Exonum is projecting to introduce Java-bindings and platform-independent interface description in the near future to make Exonum more developer-friendly.

Quorum: *An* Ethereum based distributed ledger protocol with transaction/contract privacy and new consensus mechanisms. It is a Geth fork and is updated in line with Geth releases. Quorum has changed the consensus mechanism and is aimed more towards consortium chain-based consensus algorithms. Using this consensus allows it to support hundreds of transactions per second.

Geth: Go-Ethereum or Geth is one among three original implementations of the Ethereum protocol. It runs smart contract applications exactly as programmed without the possibility
of downtime, censorship, fraud or third-party interference [7][9]. This framework supports development beyond the Geth protocol and is the most developer-friendly frame work of those
we evaluated. The transaction rate is dependent on whether the blockchain is implemented as a public or private network. Due to these capabilities, Geth was the frame work we chose to base our work on, any similar blockchain framework with an equivalent capability as Geth might be considered for such systems

TABLE II: Framework Evaluation

	Exonum	Quorum	Go-Ethereum
Consensus	Custom-built BFT algorithm	QuorumChain, IBFT and Raft-based consensus	PoW, PoS and PoA
Transactions p/s	up to 5000 transactions p/s	Dozens to hundreds	Depends
Private support	Yes	Yes	Yes
Smart Contract Language	Rust	Solidity	Solidity
Programming Language	Rust	Go, C, JavaScript	Go, C, Javascript
Decentralized	Yes	Partially	Optional

Table II shows a summary of the comparison between the three blockchain frameworks.

VI. RELATED WORK

In this section, we present **a** number of the states of the art relevant e-voting systems that use blockchain as a service. Agora [10] is an end-to-end verifiable blockchain based voting solution designed for governments and institutions. Agora uses their own Token on the blockchain for elections, where governments and institutions purchase these tokens for each individual eligible voter. A Smart Contract for

Boardroom Voting with Maximum Voter Privacy [11], proposed the first implementation of a decentralized and self-tallying internet voting protocol with maximum voter privacy using the Blockchain, called The Open Vote Network (OVN). The OVN is written as a smart contract on the public Ethereum blockchain. Digital Voting with the use of Blockchain Technology [12] proposed an integration of the blockchain technology to the current electoral system within the UK during which the voter can vote at a voting district or on an internet browser reception .Net vote [13] is a decentralized blockchain-based voting network on the Ethereum blockchain. Netvote utilizes decentralized apps (dApps) for the interface of the system. The Admin dApps allows election administrators to setelection policies, create ballots, establish registration rules and open and close voting. The Voter dApps is used by individual voters for registration, voting and can be integrated with other devices(such as biometric readers) for voter identification The Tally dApps is then wont to tally and verify election results. The main distinctive advantages of our approach over the previous approaches are the following:

a) Our approach is based private blockchain implementation. Public-based e-voting systems are inefficient concerning financial cost. This in efficiency occurs due to the high gas cost and therefore the gas limits which are set for smart contracts with in the network. Another risk using the public blockchain is that high traffic within the network, which could affect the through put of votes within the system, making it less time efficient. Moreover, a 51% attack poses a threat to a public blockchain, where any individual can sign transactions.

b) Our approach uses district-based voting. Remote voting methods such as those presented, offer no coercion resistance and therefore could lead to false election results. Moreover, web browser voting is one among the most important attack vector for hackers as they might potentially exploit voters through their own devices.

V. CONCLUSION

In this paper, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have shown that the blockchain technology offers a replacement possibility to beat the restrictions and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.

VI. REFERENCES

[1] Sos.ca.gov. (2007). Top-to-Bottom Review California Secretary of State. Available at :http://www.sos.ca.gov/elections/votingsystems/oversight/top-bottom-review/.

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

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

[4] Ajit Kulkarni, (2018), "How to settle on Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.

[5] "What Are Smart Contracts? A Beginner’s Guide to Smart Contracts", Block geeks, 2016.