Direct Democracy System Architecture for Sustainable Community Participation

Aderonke Thompson, Nikolaos Papakonstantinou, Dharmendra Sharma

Safe and Connected Society
VTT Technical Research Centre of Finland
Espoo, Finland
e-mails: ext-aderonke.thompson@vtt.fi, Nikolaos.papakonstantinou@vtt.fi, Dharmendra.Sharma@vtt.fi

***Abstract*— Active community participation without being tagged as hate speech contribution has been an established desirable element for citizens towards achieving a sustainable democratic process in communities across the world. Significant contributions to bridge this gap have been proposed by means of web technology adoption. Unarguably, in the context of free communication, anonymity is sought for serious contributions. Thus, in this paper, we examine four state-of the-art democracy platforms based on open-source technologies vis-à-vis their system architecture and features. It is observed that, while some of these platforms provide active democratic citizens participation, by e-voting, none of them adopts anonymity and full decentralization technology open-source platform in the discussion forum, which is a pivot for the waned participants' trust with the conventional centralized system that is inherently prone to single-point of failure problems; this is also prone to the vulnerabilities of data at rest, in transit and storage. Consequently, we propose a full decentralized system, based on blockchain technology that is capable of being integrated with the state-of-the-art system to ensure trust, tamper-resistance, sybil-resistance, accountability, reliability, transparency, and security, using a tokenization with the exclusive consideration of gas optimization technique to lower the cost each citizen will incur using the system.**

Keywords-architecture; anonymity; sybil-resistance; decentralization; blockchain.

I. INTRODUCTION

Governance, an outcome of citizens' choice, is evolving in organizations and communities around the world with a consensus that a good governance is quintessential for inclusion and diversity of citizens. It is a decision-making process among available options to select who governs. Of all governance types, democratic governance is the most embraced and sought after since every citizen has a platform to exercise their franchise during the electioneering process. Conversely, as laudable as the democratic governance is, the process is plagued with insincerity and mostly lacks credibility, in addition to a high cost; authors in [27] emphasize adequate fairness and transparency as a wit towards realizing a sustainable and smart governance that integrates citizens' livelihood improvement.

The following problems have been identified to be a major concern in traditional and existing electronic voting protocol:

i. the anonymity of ballot and privacy.
ii. single point of failure.
iii. inefficient authentication mechanism.
iv. votes are not universally verifiable.

Elections form the basis of governance in a democratic setting, which is the current and most acceptable type of governance that enables citizens' participation. It is a political process that requires citizens vote according to their opinion. This is done from small communities to various organizations, states, and the country at large. The process requires a high degree of trustworthiness since it is geared towards selection of capable officers that citizens deem fit for a particular position of leadership. In recent years, traditional voting systems such as paper-based voting have been heavily used, which requires voters to cast votes in appointed polling stations; the process should be transparent, secure, and reliable to ensure credibility. Since improvement is always sought, it is no doubt that advancement in Science and Technology (S&T) has impacted this increasingly evolving sphere. This advancement is principally the result of the efforts to have a secure, provable, transparent system with robust voter authentication and identification. Thus, since it is the most acceptable form of governance by citizens, advancement is incessantly sought on the overall voting system's resilience and efficiency.

E-voting is a method that digitizes voting and promises to resolve the issues and challenges related to manual voting elections on a software platform using an electronic device. Yet, the inadequacy of the e-voting systems is largely due to design flaws of centralization such as codebase, database, monitoring tools of the required infrastructure. This implies a single point of failure in secure design principles model in OWASP Software Assurance Maturity Model (SAMM) [28]. The overall impact that is beyond voters' control is that, as soon as ballot is marked and a vote is cast, the entire trust of the process lies upon the organization to ensure that there is no fraud [1]-[3]. Therefore, voters' trustworthiness become an illusion due to the non-availability of independently provable tools as anticipated by voters; that is, the degree of components compliance in relation to security characteristics as shown with its specified functionality [4], The highlighted points either hypothetically diminish voters' participation, or imposes reservations on election outcome.

Nakamoto [13] introduced blockchain technology with the development of the first cryptocurrency called Bitcoin. Blockchain stores blocks that contain a set of data such that every next block is linked to the previous one in the form of a linked list and a cryptographically secure way so that it becomes impossible to change anything in the previous blocks without rendering the blockchain invalid. It is a

 ISBN: 978-1-68558-089-6

decentralized distributed system of nodes that works in a coordinated way with the help of a consensus protocol. It is pertinent to note that blockchain technology is not sufficient to eliminate some of the susceptible vulnerabilities of e-voting such as device compromise, voter coercion, identity verification, user error as well as network attacks [16][29].

This paper explores the use of blockchain and tokenization to facilitate secure e-voting applications with the ability to assure voter anonymity, sybil-resistance, voter's eligibility, vote integrity, and end-to-end verification. This proposed system leverages fundamental blockchain features such as a self-cryptographic validation structure through hashes and public availability of distributed ledger of records that is accessible to everyone. Blockchain technology plays a key role in the domain of electronic voting due to the inherent nature of preserving anonymity, as well as maintaining a decentralized and publicly distributed ledger of transactions across all the nodes. This paper presents a detailed design of the proposed e-voting protocol, which can achieve an end-to-end verifiable, sybil-resistant and secure election process. The rest of this paper is structured as follows. Section II presents a review of the state-of-the-art architecture with related works. Section III describes the proposed system. Section IV highlights the challenges of the existing system. Section V conclusion wraps up the article with acknowledgement.

II. LITERATURE REVIEW

All the state-of-the-art platforms considered are active web applications serving many communities across the globe - DemocracyOS, Consul Democracy Decidim and D-Cent. The core and common characteristic of these platforms leverage the benefit of open-source software for cost-effectiveness, flexible and agile development processes, robust community-driven support, and easy license management. In addition, these applications hinge on the high degree of open-source community on responsiveness to information security continuous integration and deployment to fix emerging bugs.

A. State-of-the-art

DemocracyOS focuses on solving the increasing challenge of unsatisfactory expression of democratic issues through inadequate binary choices and decreasing reductionist proxies; the continuous clashing proxy representation with individual's interest, consequential crisis arisen from these issues cut across the world. Then, government insistence of citizens' exclusion from such conversations should be addressed since decisions made affect all the citizens. Because technology has a strong democratizing potential in citizens horizon; harnessing the collective wise, pluralistic views ensure choosing from pre-set options to actively designing the options dynamically.

Hence, DemocracyOS is developed to achieve construction, institutional-building, and productive participatory discussion, rather than agitation, protest and citizens taking to the streets, by making information accessible to citizens. DemocracyOS pioneered creating a link between two types of formal code, otherwise known as digital software (the net) and the legal contractual system currently operating in most governmental processes. The design is for parliaments and other institutions saddled with collective decision task; being a mix among direct and representative democracy targeting the act of voting and voting on their representative selection modality alongside these beneficiaries - Argentina netizens, non-governmental organizations as regulators, developers, and hacktivists globally for law markup language towards legislative sources data standardization [5].

CONSUL as a non-profit organization reinforces the quality, neutrality, and credibility of global citizen participation in democratic process integration with independence, transparency rule of law and inclusion. Municipalities of Madrid, Buenos, Porto Alegre New York among other institutions across 35 countries actively deploy and interact with the platform. CONSUL is designed for citizens to voice their concerns and participate through proposal development, votes for new laws, debates, crowd laws, participatory budgets, and consultations. Proposal and debates are citizen-centric considering environments are utilities that make life easy. CONSUL was a response to the 2011 15M Spanish indignados for "real democracy" demand sequel to some prevalent issues such as financial and housing crises, lack of job prospects for youth, corruption as well as lack of political legitimacy of democratic institutions [6]. The platform provides democratic processes and institution improvement by fostering a new way of citizens engagement coupled with active participation, accountability and transparency of public issues affecting the citizens. The impact of the project has continued to rise across the city of Madrid and across the world as some organizations have adopted the platform for various democratic discussions and voting processes.

Decidim contributes the societal democratization processes through the construction of technology, methodologies, practices, standards actions, narratives, and values in a collaborative and reflective way. Adoption of the platform cuts across cities and organizations worldwide such as city council, an association, NGO, a university, trade union and neighbourhood association [7].

D-Cent, an acronym for Decentralized Citizens ENgagement Technologies, an EU-funded project from October 2013 to May 2016. D-Cent is a next generation open- source, distributed, and privacy-aware tools for direct democracy and economic empowerment. D-Cent is a multidisciplinary testbed platform for emerging social movements, new models for citizen control of personal and social data in addition to privacy and security by design. D-Cent is characterized with real-time notifications about issues of concerns; policies and proposals collaborations; collective municipal budgeting and give freecoin incentives to citizens [8]. Table 1 gives the summary of the four state-of-the-art.

 ISBN: 978-1-68558-089-6

TABLE 1. STATE-OF-THE-ART PLATFORMS

Sate-of-the-art	Decidim.org	DemocracyOS	Consul Democracy	D-Cent
Purpose	It ensures participatory democracy, that is, a platform for common citizens to participate in the decision/policy by submitting proposal and this proposal can be voted for/against.	It ensures participatory democracy with Global rule of Law in 140 Countries	It ensures participatory democracy	It enables prompt information to the citizens with real-time notifications about issues of concern an open-source platform.
Source Management	Barcelona, Spain	Argentina	City of Madrid	EU
Benefits	It can be integrated with any system that requires collective, participatory decision/policy making.	It allows debate current legislation for robust public debate.	It can be integrated with any system that requires collective, participatory decision/policy making	It supports collection of various open-source tools to enable participatory governance. Some tools are blockchain based
Features	Strategic planning, participatory processes, assemblies, initiatives and citizen consultations, participatory budgeting, networked communication, accountability, equity and transparency, levels of abstraction (process and activities are separate, social contract, community	User-friendly, Collaboration between citizens and government, simple, bill tracking, Standard repository for global public documents, accountability, and civic watchdog capabilities	Customisable, secure, on-going support, proposals, participatory budgeting, debates Collaborative, legislation, incentive	Open authentication and distributed identity management, Citizen's control and data ownership, Open source and open standards, Blockchain trust Propose and draft, Decide and vote Incentivized usage
Technologies	Ruby on Rails, Vue.JS, Postgres, SQL,	GitHub is not available	Ruby on Rails, Postgres, SQL, Docker Elasticsearch	Ruby, Docker
Platform	Web	Web	Web	Web
Web Technology	Partial decentralization Web 2.0 decentralised approach to decision making,	Web 2.0	Web 2.0	Web 2.0

B. State-of-the-art Architecture

The four states-of-the-art architecture reveals the functional focus and target in a unique way that suites the stakeholders which are the citizens. Decidim and D-Cent system architecture are available from their detailed system documentation - Figures 1 and 2 respectively, it is assumed that the core architecture is tailored with the general e-voting model system-specific requirements:

i. Multi-user: a few voters can vote simultaneously.
ii. System Security: The overall system security is paramount to protect identity theft and system manipulation by outsiders or third parties.
iii. Accessibility: voters can access the system from any location using secure Internet and/or mobile devices through a web browser.
iv. Availability: the system must have high availability during an election campaign.

C. Related Works

This section elucidates existing studies stressing their motivations, objectives, methodologies, contributions to knowledge, and limitations.

[15] presents "Blockchain technology-based e-voting system". The authors stated that elections become a pertinent occurrence during democratic process, however, distrust has been the bane of electioneering process from global perspective. Some giant economies still suffer from these concerns: flawed legal system, fraudulent characterized voting system, electronic vote machine hacking, election manipulation, and booth capturing square measure are the key challenges facing the electoral system. The authors preferred the e-voting solution to the highlighted challenges. The drawback of this research is that it does not satisfy some electronic voting requirements such as anonymous vote-cast.

 ISBN: 978-1-68558-089-6

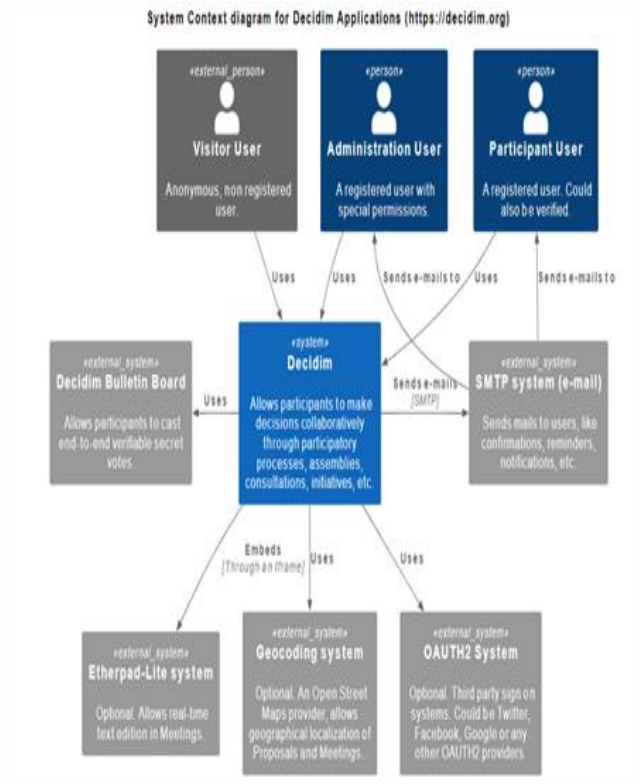

Figure 1. System Architecture for Decidim Application [26]

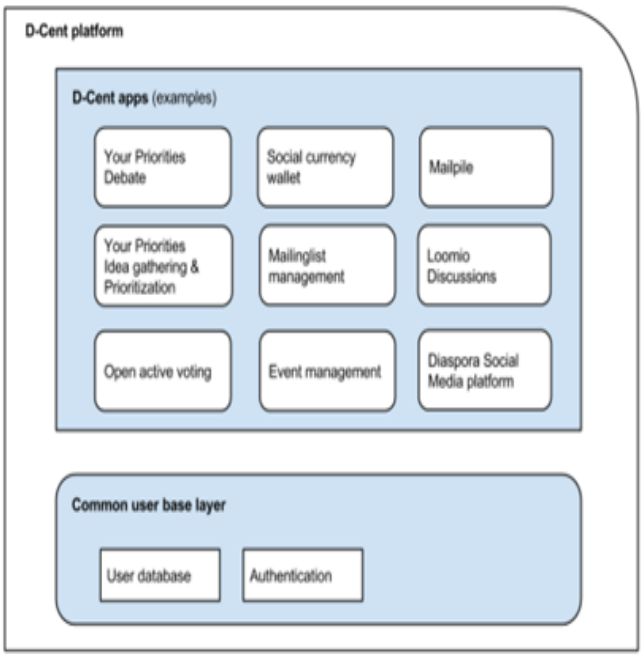

Figure 2. System Architecture for D-Cent Application [27].

[16] presents "An E-Voting Protocol with Decentralization and Voter Privacy". The focus of the study is to adopt a blockchain-based e-voting protocol that meets electronic voting requirements. Additionally, editing feature is integrated to allow voters change of mind in case it occurs within a given period. Decentralization, network peers for voters' control, and a degree of centralization is required to achieve the set objectives. Other highlights are pros and cons of blockchain adoption empirically in development/deployment and usage contexts with complex applications prospects. The drawback of this research is that there is a Central Authority (CA), as centralization point of the protocol with trustworthiness assumption. However, a malicious act from the CA brings distrust that might result to arbitrarily manipulation of cast votes for unaccredited voters; this is non-conformity to e-voting requirement.

[17] presents a "Blockchain-based e-voting approach in P2P Network". The study adopted Distributed Ledger Technology (DLT) to circumvent vote forging options plus non-repudiation and users' one-time login. Integrating the techniques with the DLT and secure e-voting user authentication in the p2p network is proposed such that trust is enhanced via vote forgery circumvention. This research was proposed because of the internet and information technologies advancement, organizations are moving from on-premise to cloud-based platforms. The drawback of this research is that a secure device is required to cast votes. Although, authors stated that the system is secure, but the system is vulnerable and susceptible to malware attacks from hackers to cast or alter vote. A major strength of the system is voter access to vote only once with no editing feature in the case of unintended errors during the voting process.

In [18], the authors explore the difficulties and uses of electronic voting procedures in elections, emphasizing the vulnerability to fraud and the demand for safe and reliable vote information. The paper advocates using blockchain technology to build a decentralized system that can validate voting data and guard against manipulation to address these problems. The decentralization of blockchain makes data backup and tracking simpler, hence maintaining the validity of the voting data. Electronic voting can use blockchain technology to increase the results' authenticity and safeguard the vote data integrity.

In [19], the authors aimed at establishing trust in the E-voting system. They examined issues with current electronic voting systems, such as fraud, a lack of transparency, and security threats like intimidation and bribery. The paper suggests a fair and transparent electronic voting system built on blockchain technology to address these problems. Therefore, their system employs a time-release encryption technique to ensure voting process fairness and a receiver-denial encryption scheme to ensure coercion resistance.

III. PROPOSED SYSTEM

Technology paradigm has continued to impact governance mechanisms and processes that culminate into a sustainable society; this study seeks to bridge the gap by adopting tokenization and blockchain technology. Electronic-voting requirements are in two parts, viz, generic, and system-specific. The generic requirements applying to general e-voting scheme, as presented by [20] and [21], include:

i. Privacy: Anyone cannot know for whom the voter voted. The ballot is hidden from outside observers.

 ISBN: 978-1-68558-089-6

ii. Individual verifiability: The ability of a voter to verify that the ballot has been counted.
iii. Eligibility: Only the legal voters can enroll in the voting event.
iv. Accuracy/Integrity: Every vote should be counted correctly.
iv. Fairness: Nothing can influence the result of voting. If the system leaks the voting result or the authority adds a voter during the voting, the event can be defined as unfair.
v. Uniqueness: Every voter can only vote once. The voter will have no permission to vote more if he votes.
vi. Robustness: Anyone.

A. Integrated System Approah

Information and data are critical to technical assessment and decision-making in a software system development lifecycle; therefore, ensuring system architecture aligns with system requirements is fundamental to achieving stakeholders concerns towards a set of consistent views and models. The state-of-the-art architectures align with the integrated system design approach [22] from the three concerned perspectives - stakeholder, system, and trades; stakeholders being the citizens, trades being the objectives and capabilities of the platforms; while system is the technology specifications deployed including security-driven constraints. In DDemo, emphasis is on system self-protection against sybil attacks, and secure system management. A rider to the integrated system approach is the state-of-the-art is compliance with the OWASP Software Assurance Maturity Model (SAMM) of people, process, and technology, it is an effective approach to system design [23].

B. System Architecture

System architecture is the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution [24][25].

Stakeholders' perspective for free speech can be handled with the system architecture in Figures 3 and 4 to integrate full decentralization into the state-of-the art.

C. Proposed System Overview

The proposed-voting protocol implements decentralized data storage using blockchain technology to make the election procedure more decentralized, transparent, and secure. There are two (2) prominent group-oriented digital signatures that support both user-authentication and anonymity which are: Group signature and Ring signature. The signatures are modern cryptographic primitives, and they provide privacy preserved authentication feature. This type of signature preserves users' privacy by granting users the ability to get verified while also hiding their identities in a group. Signatures can be generated by a user who belongs to a group by representing a group. The signer can employ other users public key without their consent to hide his identity i.e., a user adds himself into any set of his choice and produces a signature. The e-voting protocol uses the ring signatures for privacy enhancement and multi signatures to create consensus between groups, the system integrates strong identity with tokenization. and it is linked to other verified identities to improve the system authentication which is important to voting eligibility requirement and overall system security. The proposed system consists of three phases; each phase contributes to the demonstration of the system's effectiveness to achieve an end-to-end verifiable e-voting scheme that satisfies all voting requirements.

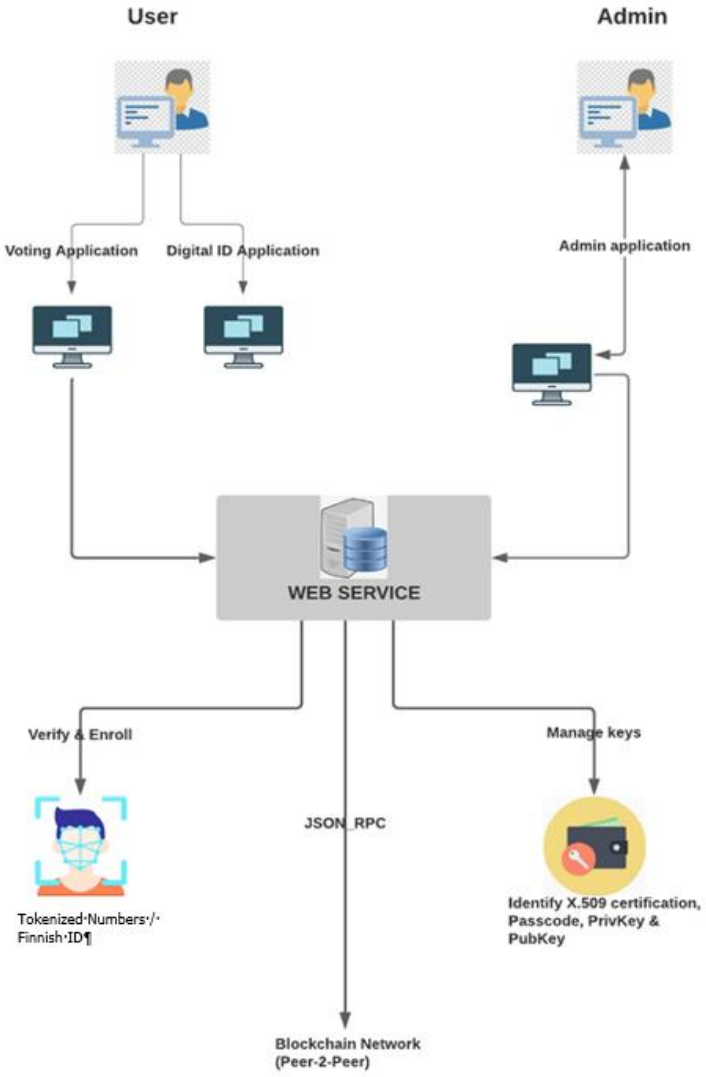

Figure 3. Proposed System Architecture.

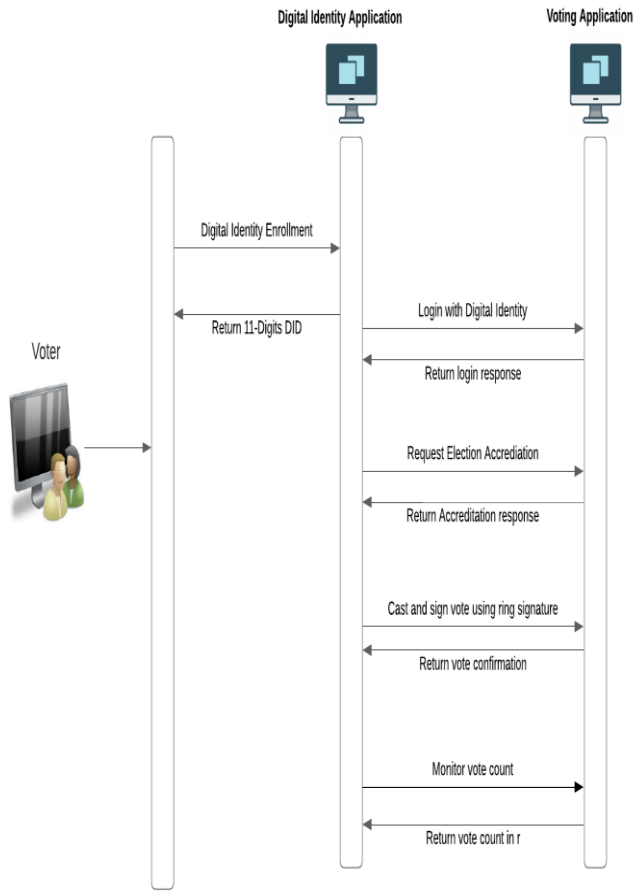

Figure 4. Proposed protocol voting phase and identity enrollment.

IV. CHALLENGES OF THE EXISTING SYSTEM

Hackers can compromise the integrity of the e-voting which is seen as a major disadvantage in the voting system. This could be done either physically or remotely where a malicious attacker changes millions of the vote data undetected. In the e-voting system, fraud is easier to perform. Identification of the voters would have to occur using participants' unique credentials such as his social security number, drive license. Perpetrators can acquire these pieces of information, logging themselves in the system and casting a vote for someone else. If someone gets a large amount of such unique identifiers with a data breach, they would be able to cast thousands of fraudulent votes. The manufacturers of these e-voting machines can be bias, causing influences in votes. Private companies who develop and distribute these e-voting systems would lock away their source code. Some companies that get hired by the government to implement these e-voting systems can act unbiased in inaccurately collecting and reporting votes. These acts do not guarantee a fair and unbiased election.

V. CONCLUSION

This paper presents the architecture of state-of-the-art platform for direct democracy participation and proposed a more secure platform with sybil resistant feature in addition to anonymity of participants using blockchain technology that meets the fundamental e-voting properties that provide full decentralization and places as much control of the process in the hands of the voters and the public. This is ongoing research; in which the system's application development is ongoing using solidity and react programming languages with gas optimization integration to ensure a lightweight feature and reduce cost for community participants. Thereafter, performance evaluation will be conducted using standard metrics.

ACKNOWLEDGMENT

The research is sponsored by the European Research Consortium for Informatics and Mathematics (ERCIM) and the host Institution – VTT Technical Research Institute of Finland.

REFERENCES

[1] D. Z. Tharindu, and K. B. N. Lakmali, Blockchain based e-voting system. International Journal of Soft Computing and Artificial Intelligence, vol. 7, Issue.1, May-2019. http://www.iraj.in/journal/journal_file/journal_pdf/4-570-15641401811-7.pdf.

[2] S. A.-B. Salman, S. Al-Janabi, & A. M. Sagheer, A Review on E-Voting Based on Blockchain Models. Iraqi Journal of Science, pp. 1362–1375, 2022. https://doi.org/10.24996/ijs.2022.63.3.38

[3] https://wentzwu.com/2021/08/02/systems-engineering-confidence-trust-and-assurance/ Accessed April 3, 2023.

[4] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers 2011 ISO/IEC/IEEE 42010 – Systems and Software Engineering – Architecture description. https://www.iso.org/standard/50508.html

[5] https://worldjusticeproject.org/our-work/programs/democracyos, Accessed April 6, 2023.

[6] https://oecd-opsi.org/innovations/consul-project/, Accessed April 6, 2023.

[7] https://decidim.org/, Accessed April 6, 2023.

[8] https://dcentproject.eu/about-us/, Accessed April 6, 2023.

[9] H. Yi, Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking, 2019 (1). https://doi.org/10.1186/s13638-019-1473-6

[10] C. Angsuchotmetee and P. Setthawong, BlockVOTE : An Architecture of a Blockchain-based Electronic Voting System. ECTI Transactions on Computer and Information Technology (ECTI-CIT), 14(2), 174-189, 2020. https://doi.org/10.37936/ecti-cit.2020142.227455.

[11] M. Bernard, The 5 Big Problems With Blockchain Everyone Should Be Aware Of, retrieved from https://www.bernardmarr.com/default.asp?contentID=1354

[12] Y. Wu, An E-voting System based on Blockchain and Ring Signature [Master's thesis, University of Birmingham]. Dgalindo, 2017, https://www.dgalindo.es/mscprojects/yifan.pdf.

 ISBN: 978-1-68558-089-6

[13] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, Bitcoin, https://bitcoin.org/bitcoin.pdf, 2019.

[14] L. Dan, Could Estonia Be the Model for Secure Online Voting?. GovTech, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/could-estonia-be-the-model-for-secure-online-voting.html, 2020.

[15] A. L. Anita, P. Junaid, P. Talif, and P. Prathmesh, Blockchain technology-based e-voting system. ITM Web Conf. vol. 32, 2020 International Conference on Automation, Computing and Communication 2020 (ICACC-2020). https://doi.org/10.1051/itmconf/20203203001.

[16] S.H. Freya, G. Apostolos, N. A. Raja, M. Konstantinos, ”An E-Voting Protocol with Decentralisation and Voter Privacy”, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). https://doi.org/10.1109/Cybermatics_2018.2018.00262.

[17] N. Shanthi, R. Suvitha, and R.C. Suganthe, “Blockchain based e-voting approach in P2P Network”, Journal of Critical Reviews, vol 7, issue 9, 2020. http://www.jcreview.com/fulltext/197-1590993271.pdf.

[18] E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan, and P. A. Sunarya, “Using Blockchain Data Security Management for E-Voting Systems”, 8th International Conference on Cyber and IT Service Management (CITSM), 2020, https://doi.org/10.1109/citsm50537.2020.9268847

[19] M. N. Neloy et al., “A remote and cost‐optimized voting system using blockchain and smart contract”, IET Blockchain. 2023, https://doi.org/10.1049/blc2.12021

[20] B. Yu et al., “Platform-independent secure blockchain-based voting system”, In: Chen, L., anulis, Schneider, S. (eds.) ISC 2018. LNCS, vol. 11060, pp. 369–386.Springer, Cham 2018. https://doi.org/10.1007/978-3-319-99136-8 20

[21] H. Tsung-Chih, W. Zhen-Yu., L. Chia-Hui, and C.Yu-Fang, “An Electronic voting system for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme”, Sage journals, vol. 9 issue. 1, 2017. http://dx.doi.org/10.1177/1687814016687194

[22] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf, Accessed April 6, 2023

[23] https://www.owasp.org, Accessed April 6, 2023.

[24] ISO/IEC/IEEE 12207:2017(en) Systems and software engineering — Software life cycle processes, 2017.

[25] ISO/IEC/IEEE 42010:2022(en) Software, systems and enterprise — Architecture description, 2022.

[26] https://docs.decidim.org/en/develop/develop/guide_architecture, Accessed April 7, 2023.

[27] H. J. Scholl and M. C. Scholl, ‘‘Smart governance: A roadmap for research and practice,’’ in Proc. IConference, 2014, pp. 163–176, https://dcentproject.eu/wp-content/uploads/2014/03/D4.2-final_new1.pdf Accessed April 7, 2023.

[28] OWASP SAMM v2.pdf https://owaspsamm.org/, Accessed November 6, 2023.

[29] R. Geetanjali, I. Razi, O. Waqar, K. B. Ali, ”On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities” IEEE Access, 9:34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411 Accessed November 6, 2023.

 ISBN: 978-1-68558-089-6