IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 May 2022, accepted 17 June 2022, date of publication 1 July 2022, date of current version 11 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3187688

Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review

ALI BENABDALLAH[1], ANTOINE AUDRAS[1], LOUIS COUDERT[1], NOUR EL MADHOUN[1,2], AND MOHAMAD BADRA[3]

[1]LIP6, CNRS, Sorbonne Université, 75005 Paris, France
[2]École pour l'Informatique et les Techniques Avancées (EPITA), 94270 Le Kremlin-Bicêtre, France
[3]College of Technological Innovation, Zayed University, Dubai, United Arab Emirates

Corresponding author: Nour El Madhoun (nour.el-madhoun@isep.fr)

This work was supported by the École pour l'Informatique et les Techniques Avancées (EPITA).

ABSTRACT To this day, abstention rates continue to rise, largely due to the need to travel to vote. This is why remote e-voting will increase the turnout by allowing everyone to vote without the need to travel. It will also minimize the risks and obtain results in a faster way compared to a traditional vote with paper ballots. In fact, given the high stakes of an election, a remote e-voting solution must meet the highest standards of security, reliability, and transparency to gain the trust of citizens. In literature, several remote e-voting solutions based on blockchain technology have been proposed. Indeed, the blockchain technology is proposed today as a new technical infrastructure for several types of IT applications because it allows to remove the TTP and decentralize transactions while offering a transparent and fully protected data storage. In addition, it allows to implement in its environment the smart-contracts technology which is used to automate and execute agreements between users. In this paper, we are interested in reviewing the most revealing e-voting solutions based on blockchain technology.

INDEX TERMS Authentication, blockchain, e-voting, privacy, security, smart-contracts, transparency.

I. INTRODUCTION

In recent years, remote electronic voting (e-voting) has emerged to increase voter turnout while allowing everyone to vote without the need to travel. On the one hand, the abstention rate has been steadily increasing, largely due to the need to travel to vote. On the other hand, in many countries, the transparency of elections is increasingly challenged and undermined [1]. Moreover, it seems relevant, even necessary, to rethink the protocols of current voting systems to make them more transparent, inclusive, and close to citizens while maintaining a maximum level of security. Therefore, the application of blockchain technology to ensure e-voting appears to be an interesting prospect to meet these challenges.

Indeed, Internet voting has already been implemented in several countries for small-scale elections, but it is still hesitant. The risks of attacks are too important and the low scalability of such voting processes does not yet allow to consider it for national elections. The process remains, like paper voting, very complicated to verify and audit for a citizen who has no control over the voting system. To overcome these problems, blockchain appears to be a promising technology [2]–[4].

Blockchain is an emerging technology whose full potential has not yet been realized and on which more and more applications are being built. It was first used to exchange cryptocurrency with the creation of the Bitcoin system in 2008. Due to its decentralized, anonymous, and secure nature, it has been used in many projects that required a technology to store and exchange information without going through a Trusted Third Party (TTP) [5].

In this paper, we are interested in reviewing the most revealing e-voting solutions based on blockchain technology to understand their particularities and what they can bring compared to traditional voting. Our approach is as follows: we gathered as much information as possible about the state of blockchain technology applied to e-voting from research papers published between 2010 and 2021. Then,

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

we extracted several properties shared by most blockchain-based e-voting applications. In doing so, we defined a subset of comparison criteria by grouping them (the extracted properties) into 4 themes: voter authentication methods, voting encryption/hashing algorithms, resistance to attacks, security properties.

This paper is organized as follows. Related works are introduced in section II. In section III, we briefly present what is blockchain technology. In section IV, we compare the blockchain-based e-voting applications within several categories while in section V, we expose the limits and issues raised by this technology for e-voting applications. In section VI, we discuss considerations, experiments and ongoing projects for e-voting with or without including blockchain technology. The last section concludes the paper.

II. RELATED WORKS

To take advantage of the benefits of it, blockchain technology was recently proposed as a new technical infrastructure for the development of several types of IT (Information Technology) applications, including e-voting applications. Indeed, although the principle of e-voting is considered as an old concept, it has now become a viable solution with the democratization of blockchain technology. The authors of the paper [6] wrote an empirical review of e-voting applications using blockchain technology. They began by establishing the challenges that e-voting applications face: privacy, lack of evidence, fraud resistance, ease of use, scalability, speed, and cost. They compared a set of e-voting applications that they believed covered all aspects to create a robust system. They did this by comparing 14 applications on 6 properties, indicating in a table whether and how each implementation met each criterion. Indeed, there were not enough criteria in this paper to compare all the specifics of e-voting applications. The approach inspired our paper, but we expanded the list of specifics and did our tables differently.

The paper [7] is based on using a technique called ''systematic mapping'' introduced in [8]. It is organized around five research questions whose answers, according to the authors, cover the entire scope of their review: (1) What are the current e-voting system gaps ? (2) Can the blockchain concept improve e-voting systems ? (3) What are the research topics and proposed solutions that have been published in blockchain-based e-voting ? (4) Which blockchain platforms/consensus models are used? (5) What are the future research directions for the blockchain-based e-voting system? They have answered all these questions and more specifically question (3), which focuses on comparing between e-voting applications that are based on blockchain technology. They classified these applications into 5 categories, where each category represents the main purpose of the application or its main feature. This classification is not enough and it is not based on an obvious comparison between the applications. In our paper in hand, we extracted several properties shared by most blockchain-based e-voting applications, and then we defined a subset of comparison criteria by grouping them (the extracted properties) into 4 themes and hence 4 tables.

The authors of the paper [9] described the use of blockchain-based e-voting applications in real-world scenarios. They then extracted a set of properties that a blockchain-based e-voting application should satisfy to be a fair, transparent and democratic election system. These properties are public and individual verifiability, dependability and reliability, consistency, auditability, anonymity, transparency, scalability, eligibility, authentication, and fairness. Subsequently, they compared 8 blockchain-based e-voting systems, highlighting their respective strengths and weaknesses compared to previously established properties, and they proposed some improvements.

Our paper used a similar methodology and objective to those published by the authors in the paper [10]. The analysis of the subject proposed in this paper is very interesting and our work is in line with it. Otherwise, our work differs from the latter and thus brings a new approach to the topic of blockchain-based e-voting. Indeed, our work complements the paper [10] since we propose about thirty additional references in the comparison of implementations. We have been able to use more recent papers and have used a more inclusive selection technique than the one proposed in [10]. In the latter, the authors identified several exclusion criteria that we did not apply in the preliminary search, allowing us to study other relevant papers. In addition, we relied on other published literature reviews that reference and compare voting applications. This allowed us to gather outside opinions, both positive and negative, on articles proposing voting applications, and thus gain credibility. While the overall approach to the systematic literature review is similar, the criteria for comparison differ for some. In our paper, section IV-A details the voting process proposed by each voting application. Moreover, section IV-B compares the voter authentication methods, which is not specified in [10]. These differences make it possible to compare differently and more widely these e-voting implementations and thus bring novelty to the field of e-voting with the blockchain.

Our paper provides a more complete and richer comparison. It is designed as a guide for any research on the subject. Our paper not only compares the existing solutions but makes it easy to customize solutions based on specific criteria that are crucial for e-voting. We have determined a set of criteria that we have deemed very specific to include as many blockchain-based e-voting applications as possible in our comparison. In this way, our proposed work should help the community to focus on certain criteria and to compare the proposals of several applications as well.

III. BLOCKCHAIN TECHNOLOGY

Blockchain is a form of distributed ledger where participants can store and exchange information directly with each other without the need to know or trust each other's beforehand. A blockchain implements the concept by aggregating records into blocks of data that are cryptographically signed to

prevent data tampering. The usual method is to create a hash of the previous records and insert in the header of the next block of data. Thus, each block depends on the previous one and any attempt to modify a record in the chain would modify the hashes of the blocks down the chain. For the participants to identify valid records chain and guarantee integrity of data, participants of a blockchain must agree on a **consensus protocol** [5].

Bitcoin blockchain uses a **Proof-of-Work** consensus. Each miner will try to reverse the hash of the previous transactions to gain a reward. Reversing a hash is a computationally heavy operation, but verifying it is very easy and so it would be impossible to fake a hash and have all the nodes agree on it, unless one owns more than 50% of the computational power of the miners [11]. **Proof-of-Stake** is a protocol that does not need a lot of computational power where miners are randomly selected by how many coins they dedicate to be a miner. These funds are stored and can be taken back. However, mining power would also increase with wealth which would mean that the biggest coin owners could centralize the blockchain [12].

To make trusted applications, the consensus protocol of the hosting networking. The paper [13] draws a comparison table between different consensus algorithms and their malicious nodes tolerance. A Proof-of-Stake algorithm has a tolerance of 51%. As an indicator, which is currently using a Proof-of-Work algorithm and will upgrade as a Proof-of-Stake with Ethereum 2.0 has 57.2% of its coins stored in the top 10000 wallets.

The blockchain mainly differs on what consensus protocol they are implementing. These protocols usually also define the permission degree of a blockchain. That means what operations participants can do on the blockchain. A blockchain is called public when any entity can read, and permissionless if such entities can also write. There is usually a trade-off between permissions/centralization and scalability. A blockchain with restrictive read/write policy where the authentication of data is left to a few trusted nodes is generally more efficient than a public and permissionless blockchain as the consensus is easier to reach. However, blockchain's goal is to decentralize governance to make trusted data transactions and applications so, depending on the use, a compromise must be made between decentralization and efficiency [5], [14].

Blockchain 2.0 is born from the ability to make decentralized applications with smart contracts. Nick Szabo first defines a smart contract in [15] and describes it as a computerized transaction protocol that executes the terms of a contract. Blockchain smart contracts were first implemented in Ethereum by Buterin in [16] that was designed like a decentralized computer that supports Turing-complete scripts. The paper [17] describes Ethereum, its limits and its functionalities, including its potential use as a support for issuing tokens.

Blockchain is evolving toward 3.0 as technology improves and decentralized applications are developed. The authors of the paper [18] propose a survey of the different new usages of blockchain 3.0 including e-voting where blockchain brings new solutions to the problem.

IV. COMPARISON

In the following, we compare the proposed blockchain-based e-voting applications based on the following five main thematic categories: (A) implementations used, (B) voter authentication methods, (C) voting encryption/hashing algorithms, (D) resistance to attacks and (E) security properties.

A. IMPLEMENTATIONS USED

The different blockchain-based e-voting applications share the same overall voting process, from voter registration to the announcement of the result. In this section, after briefly stating the general operation of e-voting with blockchain technology, we develop some technical features of the different implementations.

1) STEPS OF THE E-VOTING PROCEDURE

- Initialization (Phase 1): during this phase, the smart contracts are initialized with the voting rules, the list of voters and the list of candidates. Any subsequent modification of this phase must be made according to these initial smart contracts. For applications where the voter must register or confirm his registration, this is done in this phase [19]–[22]. In many other papers, registration is not required because a central authority sends its keys to all voters [23]–[27].
- Identification (Phase 2): on the day of the election, the users connect and identify themselves thanks to the different authentication mechanisms presented in section IV-B. Sometimes a dedicated website or application is used [21]. It is not recommended to use a cell phone to vote because they often hide malware.
- Voting (Phase 3): once identification is well done, the voter chooses one or several candidates according to the voting rules. The vote is then encrypted using an encryption algorithm or hashed using a hash function (see section IV-C). The encrypted or hashed vote is finally added to the blockchain. Indeed, this vote is invisible and irreversible in many cases. The authors of the paper [28] propose a solution which allows to perform a second vote to modify the first one. The solution presented in [29] proposes to rank several candidates and applies the Borda counting method [30] in the counting phase. The e-voting application presented in [24] allows the voter to withdraw its vote before the deadline. In the paper [31], a ballot is broadcast containing the vote but can only be decrypted once a sibling block is broadcast at the end of the voting phase. The authors of the paper [32] also propose an abstention vote.
- Counting (Phase 4): when the end of the election is declared, it becomes impossible to change or add votes. If the counting process takes place in parallel with the voting, it is essential that the current score is not visible to anyone to avoid influencing voters who have

not yet voted. It is during this phase that any audits take place to ensure that no fraud has been committed (see section IV-E).
- Results (Phase 5): through a secure channel, the results are announced in detail and made accessible to all.

2) TECHNICAL FEATURES

The consensus protocol is an essential feature of the solutions. The papers [26], [27], [33]–[52] propose solutions on the Ethereum blockchain that supports smart contracts. These smart contracts work like a public ledger and are used to both record and tally votes. They guarantee privacy and can support custom encryption methods. However, smart contracts on Ethereum suffer from scalability issues that can be solved by deploying them on a less decentralized network. The authors of [53] [54]–[60] propose solutions using smart contracts on Hyperledger Fabric that can hold up to 100000 transactions per second [53]. Two papers [61], [62] propose using Bitcoin as a blockchain implementation for e-voting. Bitcoin is a well-known open-source blockchain-based cryptocurrency.

The use of blockchain technology cannot completely erase the presence of a central authority administering the vote. In addition, a public blockchain could hardly run a nation-wide election due to scalability issues. Many solutions offer a partially centralized blockchain. The architecture solution proposed in [32] is designed with three levels of nodes: national, constituency and local. The local level consists of all digital polling stations and is associated with a constituency node. Constituency nodes hold a subset of local stations and are connected to national level nodes that add blocks to the blockchain. In this same paper as well as in [63] and [64], each candidate has a dedicated chain where the first transaction is the name of the candidate and every other transaction are votes for him. A vote can be seen as a transaction and each block contains the hash of the previous block and the Merkle tree's root. A transaction must contain the voter's ID, his signature, his vote, and a timestamp.

TABLE 1. Voter authentication.

Voter Authentication (Registration)	Papers
Phone Number (MSISDN)	[22]
ID Document	[20], [21]
Validity of Credentials (Public/Private key)	[19], [21], [23]–[27]
Biometric Identification	[29], [31], [65], [66] [46], [67]

B. VOTER IDENTIFICATION METHODS

As we illustrate in Table 1, one of the categories we were able to isolate is the voter authentication methods. Indeed, several authentication methods for the voter have been proposed in the papers of blockchain-based e-voting applications. There are papers that fully detail the authentication method while others only mention it very quickly, which is a problem. The issue of voter authentication is fundamental to ensure that votes are not stolen, sold, or extorted. One of the biggest problems with e-voting is that we cannot guarantee good voting conditions, such as the perfect confidentiality of a voting booth. To reduce the impact of this loss of confidentiality, it is important to ensure that the person voting is who they say they are. The different methods of authenticating a voter are classified as follows (see Table 1):

- Authentication with the Mobile Station International Subscriber Directory Number (MSISDN).
- Authentication with a scan copy of an ID document: ID card or Passport.
- Authentication thanks to the validity of credentials: match between private key and public key [81].
- Biometric authentication: it uses the fingerprint, the iris of the eyes or facial shape(criteria that can be combined).

For national elections, the only use of the **phone number** to authenticate voter identity is presented in the paper [22]. This method of authentication does not allow people who do not have a phone subscription to access the vote. It also creates significant security holes by relying on private telephone operators to obtain citizens' numbers.

Concerning authentication with an **ID document** [20], [21], this poses security and scalability problems. Indeed, it is necessary for the system to quickly process the scanned copies of millions of users and verify that the identity documents correspond to each user. If this verification is automated, it can be very complicated to implement at large scale. In addition, the scanned copy would have to be taken instantly to ensure that it is not a fraud. Therefore, a more reliable and faster method of authentication should be considered.

The most common authentication method in blockchain-based e-voting applications is the **matching of a private and public key pair**. The Elliptic Curve Digital Signature Algorithm (ECDSA) is very often used [23]–[25]. It allows to efficiently ensure the conformity of a vote cast by a user without revealing his private key. This asymmetric cryptographic mechanism is commonly used in blockchain applications because it meets many security criteria (see section IV-E). Nevertheless, this method reaches a limit that is not negligible: the possibility of selling or stealing the private key of a user. Indeed, nothing prevents a user from selling his private key to a person or an organization that could cast a large amount of votes with impunity. Another problem is the loss of the password. If a voter loses his password, it is very complicated to assign another one securely. A hacker could change the user's password without his knowledge, which would be very problematic. The authentication by public/private key is therefore not perfect and brings the possibility of another stronger method: **biometric authentication** [82].

The research papers [29], [31], [46], [65]–[67] propose the use of biometric authentication method for the voter at the time of voting. This proposal seems indeed very interesting to deal with the key exchange problem mentioned above. The fingerprint or iris photo of the eye forms a user-specific hash key that is much more secure than an emailed code. This greatly reduces the risk of fraud and ensures that a user who

TABLE 2. Encryption or hashing of the vote.

Encryption/Hash Algorithms	SHA-256 Function	Homomorphic Encrpytion	Zero Knowledge Proof	Blind and Ring Signature	Ethereum Hash Function (Keccak-256)
Papers	[19], [23], [24], [63], [65]	[19]–[21], [25], [68], [69] [20], [41], [43], [45], [52], [70]–[73]	[20], [33] [38], [41], [43], [45], [49], [56], [58], [62], [70], [74]	[26], [75] [28], [76] [25], [44], [49], [52], [57], [67], [73], [77]–[80]	[22], [26], [26], [27], [33]–[35], [64]

votes is who he claims to be. Nevertheless, the major problem remains the logistics that this requires on a large scale: each voter would have to have a device that allows the transmission of his biometric data, which seems difficult to achieve now.

If the security of voter authentication seems complicated to ensure for the moment, the European initiative through the eIDAS regulation seems to be an interesting perspective to secure the identification of the voter during an e-vote [83]. The eIDAS regulation applies to electronic identification, trust services and electronic documents. It aims to establish an interoperability framework for the different systems set up within the EU Member States to promote the development of a digital trust market. The regulation defines the requirements for the mutual recognition of electronic means of identification and electronic signatures for exchanges between public sector bodies and users.

C. VOTING ENCRYPTION/HASHING ALGORITHMS

Once the user is identified, his vote must be added to the blockchain while preserving his anonymity. It is at this point that the vote encryption/hashing algorithms intervene to ensure security and integrity of transactions during the election. As illustrated in Table 2, there are different functions that can hash or encrypt the vote at different levels. One of the most used is **SHA-256** [23], [24], [63], [65]. SHA (Secure Hashing Algorithm) is a cryptographic hash function that produces a 256-bit hash value consisting of 64 hexadecimal characters. It was designed by the United States National Security Agency. SHA 256 is a new hash function that does not have collusion problems and seems to be reliable now [88]. The advantage of this algorithm is that it accepts any input length and produces an arbitrary output length, whereas most other algorithms produce a fixed output length.

The **Homomorphism** encryption property allows to operate on ciphertexts without decrypting them [25]. In the case of a voting system, this property allows encrypted ballots to be counted by a third party without any information contained in the ballot being disclosed. Typical homomorphic cryptosystems applied in a voting system are Paillier encryption (unbounded number of modular additions) and ElGamal encryption (unbounded number of modular multiplications) [20], [21]. The homomorphic encryption was also applied in the e-voting system presented in [69].

The **Zero Knowledge Proof** is often used in a voting system [20], [33], [38], [41], [43], [45], [49], [56], [58], [62], [70], [74] to prove that the statement is indeed what it claims without revealing any additional information about the statement itself. In a voting system, the voter must convince the authority that his ballot is valid by proving that the ballot includes only one legitimate candidate without revealing his vote.

Blind Signature and Ring Signature are very useful to provide the user's anonymity and the signer's privacy [89]. Voting systems use blind signature to convince the tallying center that the ballot is from a valid voter, without revealing the owner of the ballot [26]. Simultaneously, the authority signing the ballot learns nothing about the voter's choices. In blind signature, both voters and tallying center must trust the signer. If the signer is compromised, the signature scheme may stop working. Unlike blind signature, linkable ring signature is proposed to avoid untrusted signers. It is a cryptographic process that allows a person to electronically sign his vote in an anonymous way [28], [76]. This mechanism involves other users chosen by the author of the signature (the signer) who are not necessarily informed of their participation in the creation of the electronic signature. When the voter signs the ballot, he must include the public keys of other voters to make his signature indistinguishable from those of other voters. By comparing the linkability tag, the authority can easily tell if that voter has already voted. Nevertheless, to be reliable, these methods require anonymous channels and trusted signing institutions.

For e-voting applications that are based on the Ethereum blockchain, they use an **Ethereum-specific Hash** function that can be added to other encryption algorithms [26], [27], [33]–[35], [64].

D. RESISTANCE TO ATTACKS

The resistance of a voting system to external attacks is obviously very important. Some of the papers we have studied mention the possibility of resisting certain attacks, although it is impossible to assert that an application is completely secure against all cyberattacks. Indeed, if such an application has not been tested on a large scale, it would be very difficult to predict all possible threats. Therefore, in this section we will only mention the papers whose application is specifically protected against one or several attacks

TABLE 3. Resistance to attacks.

Attack/Threat	Application is resistant	Application is not resistant
DDOS	[21], [26], [26], [27], [34], [35], [63], [64] [44], [72]	[22], [28], [33], [53], [84] [25], [50], [58], [77]
Sybil Attack	[21], [25], [27], [63]	[28]
Man of the Middle	[44], [53]	-
Byzantine Fault	[20], [25], [27], [31]–[33], [63], [75]	[22]
Coercion	[21], [26], [31] [39], [74], [80], [85]	[20], [26]–[28], [33], [53] [33], [40], [41], [45], [50], [60], [78], [86]
Brute-Force Attack	[23], [87]	-

(first column of the Table 3). Otherwise, some papers point out the weaknesses of certain applications in the face of these same attacks (second column of the Table 3).

DDoS (Distributed Denial of Service) are one of the most critical challenges facing cyber-attack experts today. Many e-voting applications using blockchain claim to face this type of attack [21], [26], [27], [34], [35], [44], [63], [64], [72]. The distribution of the service across different nodes, which is possible with a blockchain, appears to be a solution to the DDoS attack because it is almost impossible for the adversary to compromise all the servers. If a DDoS attack occurs, the system will continue to operate without any interruption due to its distributed nature. Since blockchain nodes work together independently, the architecture of these e-voting applications is designed to avoid single points of failure.

Some texts mention a possible resistance to the **Sybil attack** [25], [27], [63]. These different approaches to Sybil attack prevention are identity validation, social trust graph algorithms, economic costs, personhood validation, and application-specific defenses. However, as mentioned earlier, the possibility of generating new identities does not seem to be excluded, especially if the authentication system is fragile. In such an attack, the attacker bypasses the reputation system of a peer-to-peer network by creating a large quantity of identities and using them to have a disproportionate influence, which, in the case of a vote, is dramatic. Such an attack could distort the outcome of the election and elect someone to lead the government that the people would not have chosen.

Regarding the **MITM** (Man-In-The-Middle) attack, only two papers [44], [53] state they are resistant (see Table 3). The other papers do not mention that it resists this type of attack and this is because the intrinsic properties of the blockchain allow the resistance to this attack in an automatic way as follows: since voters and smart contracts both sign their messages and voting data are encrypted, an adversary cannot forge the signature or change the data of the parties involved in the transactions. The public keys used for signature verification are all visible in the blockchain, which prevents the adversary from deceiving the parties. It is indeed impossible to replace the original public key with the opponent's without being seen. The encryption of the ballot also eliminates the possibility of the ballot being leaked.

The **Byzantine fault** occurs when some of the interlocutors (voters) are unreliable and can change the rules (or consensus) of a voting process. Many e-voting applications [25], [27], [32], [33], [63] are Byzantine fault tolerant. This means that no node in the network can influence other nodes about the consensus. Furthermore, the nodes do not have the authority to change the consensus order once it is reached.

The **Coercion-Resistance** occurs when a voter cannot cooperate with a coercer to prove to him that he voted in a certain way. Such a system ensures that the coercer cannot be convinced of how a voter is voting, even if the voter cooperates with the coercer. As illustrated in Table 3, apart from a few exceptions & [21], [26], [31] [39], [74], [80], [85], several applications are susceptible to this type of attack [20], [26]–[28], [33], [40], [41], [45], [50], [53], [60], [78], [86] because it is impossible to prevent a user from voting in front of someone else or selling his key. This is a major flaw of e-voting that is unfortunately almost impossible to overcome today. Therefore, the criterion of **Forgiveness** has emerged as a more reachable goal than pure coercion-resistance. Forgiveness is the ability of a voter to change his vote after it has been cast. This allows the coerced voter to change his vote later, once the attacker thinks he has voted a certain way.

Concerning the **Brute-Force attack**, few papers like [23] and [87] specify that they resist it. We can therefore assume that other applications do not claim to be protected against such an attack. A brute-force attack consists in trying a maximum of passwords to enter the system and thus to commit a vote. The size of the key is then very important since it directly influences the complexity of such an attack.

E. SECURITY PROPERTIES

A voting system needs to be reliable whether it is paper voting or online voting. Not only will malicious users always try to influence the vote and attack from any breach they discover, but also, for legal reasons, it is necessary to provide evidence to the losers that they lost the election [4]. In this section, we will define the minimum-security properties that any voting system should have. Table 4 presents the applications that meet these various criteria.

Most of the proposed solutions present the **Audit** property as the most fundamental one to check if the system provides a proof that all its parts work as expected. Indeed, most systems use several layers in their decentralized applications. Not only is it required that the reports of each layer be verifiable,

TABLE 4. Security properties.

Properties	Papers
Audit	[20]–[26], [26]–[29], [31], [32], [34], [35], [53], [63]–[66], [68], [75], [84], [87], [90]–[92]
Voter Verifiable	[19]–[26], [26]–[28], [31]–[35], [53], [63]–[65], [68], [75], [76], [84], [87], [91], [92] [20], [40], [41], [43]–[45], [47], [49]–[52], [57]–[60], [62], [74], [80], [85], [93]–[97]
Vote-Alterable	[21], [24]–[26], [26], [28], [33], [35], [66], [76], [90]–[92]
Integrity	[19], [21]–[26], [26]–[29], [31]–[35], [53], [63]–[66], [68], [75], [76], [84], [87], [90]–[92] [36], [38], [39], [48], [60], [77], [78], [96]
Privacy	[19]–[26], [26], [28], [29], [31]–[35], [53], [63]–[66], [68], [75], [76], [84], [90]–[92] [33], [38]–[41], [43], [45], [49], [51], [55], [58], [70], [72], [77], [79], [93], [95]–[98]
Confidentiality	[19]–[23], [25], [26], [26], [27], [29], [31]–[33], [53], [63]–[66], [66], [68], [75], [76], [84], [90]–[92]
Fairness	[21], [26], [26], [27], [29], [31]–[33], [53], [65], [68], [75], [87] [40], [44], [50], [52], [70], [78]–[80], [95]
Eligibility	[19], [21], [22], [24]–[26], [26], [27], [29], [31]–[35], [53], [63], [65], [66], [68], [75], [76], [84], [87], [91], [92] [20], [39], [40], [42], [48], [50], [51], [57], [61], [67], [74], [78], [80], [95], [97]
Transparency	[22], [26], [27], [31], [33], [34], [53], [84], [87], [91]
Receipt-freeness	[20], [25], [28], [37], [40], [41], [45], [53], [62], [66], [74], [76], [78]

which would mean that the system is auditable, but also to always verify them, which would make the system audited. The paper [31] keeps tracking of the whole voting process, including rejected votes. Moreover, employing smart contract gives more trust to the audit as the code cannot be tempered.

The **Voter-Verifiable** property is complementary to the audit property. A user must be able to verify that his vote has been correctly cast and counted. It can detect attacks that the audit property cannot. For example, if a hacker finds a user's private key, he may vote on behalf of someone else, which would not be detected by the audit property and could only be detected by the actual voter. The paper [53] proposes a solution where anyone with access rights to the blockchain can verify that his own ballot has been recorded and that every ballot has been recorded correctly.

Let us suppose a voter realizes that his vote was not counted correctly, how would he be able to prove it ? The **Vote-Alterable** property gives a user the ability to alter his own vote. In this way, it will not be the responsibility of the user to contest his own vote without any need of proof. The paper [26] labels it *Forgiveness* property and states that it is also a weaker property of resistance to coercion, since a coercer could not be sure that the coerced citizen would not change his vote.

Data **Integrity** is an intrinsic property of blockchain technology. [5] states that *Data Distribution*, *Data Replication*, a *Cryptographic layer*, *Data Transparency* and *Data Immutability* are default properties of a blockchain. It guarantees that data must never be altered during transmission or processing, either intentionally or accidentally. In the case of an application, it is also necessary to verify that a vote is not counted twice.

The **Privacy** property is necessary to protect users from having their personal information leaked. In most systems, a pair of login and passwords are provided by a central authority, which holds all the voters' private information. The central authority could be the government who already has all our data. Other systems require a registration however it is vulnerable to Sybil attacks and hacking. People could choose a password that has already leaked and a hacker could usurp their identity or register from a hacked terminal. It is also necessary to protect the data of each vote that, in this paper, we call confidentiality.

The **Confidentiality** is one of the most important properties. A voter should never be identified from his vote. A vote will always be decrypted so if a vote link could be made between a vote and a voter, it would be possible to identify who voted for whom. It is primarily designed to protect voters from any coercion but also from any repercussions caused by their vote. A system that does not fulfill this property could be used by an authoritarian government and give it the ability to identify those who voted for the opposition, which would not only put them at risk but also deter people from voting against them. The paper [68] labels both privacy and confidentiality properties as privacy. Not only does the system protect its users' data but it also encrypts the vote and does not give any receipt.

The **Fairness** property means that the election results are not counted in real time. This way, no one should know which candidate is ahead in the election and other voters will not be influenced. The paper [26] proposes to divide the vote by phase and the tallying phase only starts once the election has concluded.

The **Eligibility** property states that only the eligible voters can cast a vote. This property cannot be strictly fulfilled in a remote e-voting solution because it requires an Internet connection and a computer to vote. Not everyone has such equipment and some people still need to discover new technologies, but we can consider that this problem will be solved in the future. Some systems require people to buy a token to vote or pay a high transaction fee, which would discourage people from voting. The paper [33] proposes a solution where the administrator has a list of all the eligible actors however it uses Ethereum that has, in 2021, very high transaction fees as the network is saturated. We still consider that this solution guarantees the eligibility property as upcoming upgrades of Ethereum will lower the transaction fees of the network.

Indeed, the **Transparency** of the whole voting process is also a necessary property. An open-source code is always better, especially when it is from a smart contract because of smart contract's transparency properties. On the one hand, it adds transparency to how data are handled and how security flaws can be reviewed by peers. On the other hand, it adds reliability and robustness to the application. The paper [91] is verifiable as its code base is open source. Nevertheless, while transparency allows flaws in a system to be revealed

and resolved through the reviews of researchers and computer scientists, it also opens the door to malicious actors who could more easily detect security flaws. Transparency can therefore increase the vulnerability of a system as shown by the example of the Swiss Post in 2019 which temporarily published the source code of its voting system [99].

The **Receipt-Freeness** property is intended to prevent vote buying where an elector cannot construct a receipt to prove to a third person that he voted for a certain candidate [40].

V. LIMITS AND ISSUES

In the previous section, we presented and compared the different existing e-voting applications using blockchain technology. If blockchain technology brings hope, many researchers nevertheless claim that e-voting remains dangerous and does not significantly increase the turnout rate [4], [100]–[103]. Blockchain is indeed not a miraculous solution to all the problems that e-voting faces. It is therefore relevant and necessary to mention the limits of blockchain for e-voting applications. In this section, we expose the limitations and problems that these applications share, for further research in the field of e-voting applications.

A. SCALABILITY

Although there are many proposed e-voting applications using blockchain in theory, only a few have been implemented and they have only involved small-scale elections as in Sierra Leone [104]. In fact, **Scalability** is one of the major challenges of e-voting since the system must be able to handle millions of votes in a limited time. The problem is that it is difficult to predict the maximum number of simultaneous votes that the system should be able to handle without crashing. Reorganizing an election after a crash would be expensive and would not prevent the problem from recurring. One possibility would be to organize ''voting slots'' where each citizen would only be allowed to vote for a certain time interval. This would again pose problems of anonymity and increase the complexity of the algorithms during registration and authentication.

B. GENERAL WEAKNESS: UNPREDICTABLE ATTACKS

Although some applications claim to be prepared for certain attacks (see Table 3), it is impossible to be prepared for all eventualities [4]. A large-scale attack could be carried out during an election and would have dramatic consequences. Indeed, the attacker could rig the vote if he manages to generate his own keys or publish the votes by linking them to their voter. This could lead to an unprecedented crisis and would cause voters to lose confidence in the system. Therefore, e-voting, even with blockchain technology, still poses major security issues that cannot be avoided for sure.

C. LACK OF SECURITY FOR THE VOTER IDENTIFICATION

The weakness of the identification system is a major difficulty. Without the use of a Biometric system to ensure the authentication of the voter (see Table 1 and section IV-B), it is impossible to be totally sure that the vote is cast by the right registered person. This flaw is important because it can lead to democratic abuses, especially in case of theft or sale of authentication keys. If an organization or company wishes to interfere in an election, it could organize an illegal sale of voting keys to gather many votes and vote in place of the people who sold their votes. These voters, disillusioned with the representative system and traditionally abstainers, would have the opportunity to make money by not voting. This would be a disaster for democracy because the richest people could take power. Vigilance must therefore be maximal on this aspect of e-voting.

D. DECENTRALIZATION AND EFFICIENCY

There is an intrinsic debate about blockchain that brings real challenges. While decentralization is at the heart of the project, to build trust in the voting system and avoid the involvement of a corrupt third party, such an application must also be efficient. There is therefore a **paradox**: we want both the advantages of a decentralized system, while retaining the properties of a central authority to manage the vote [4]. Such a utopia is impossible. In any case, it must be admitted that some centralization is necessary to organize a national election. But then, hacking of the central authority is made possible and can have very bad consequences on the vote. It is therefore essential to realize that blockchain does not solve, despite its decentralized nature, all the problems related to e-voting.

E. DIGITAL DIVIDE

It is important to mention the current problem of the digital divide [105]. If such an election is to be held, it is necessary to set up e-voting machines in all cities to allow all citizens, including those who do not have a computer or a compatible phone, to vote. Indeed, many elderly and low-income people are excluded from the process of digitizing public services. Without a real democratization of digital technology, a significant proportion would not be able to vote, which would therefore be discriminatory. Future e-voting applications must therefore be aware of this problem.

F. NEW PROBLEMS WITH BLOCKCHAIN TECHNOLOGY

The paper [4] presents new issues raised using blockchain technology for e-voting applications.

Blockchain is designed to be decentralized and managed by multiple actors. This means that blockchain protocols require governance and coordination, which can be difficult to manage. Hence, the blockchain technology introduces more complexity into software and into its management as well. This additional complexity causes problems in fixing bugs and deploying new software. Because a decentralized system does not have a single point of control, any protocol change, even to fix vulnerabilities, requires coordination. The advantage of the blockchain thus becomes its disadvantage: it takes longer to address security flaws in a decentralized system than in a centralized one. Blockchain systems can be

vulnerable for longer periods of time than their centralized counterparts. The ability to quickly fix bugs is a priority for a voting application, but the blockchain technology cannot ensure it.

Another problem is that the use of new consensus protocols or cryptographic primitives is strongly discouraged if they have not been thoroughly tested by the industry first. The papers [106] and [107] illustrate that distributed consensus protocols and cryptographic systems are difficult to implement properly.

G. CHALLENGES RELATED TO BUGS IN SMART CONTRACTS

Decentralized applications using smart contracts pose new security challenges. Indeed, vulnerabilities in smart contracts have been exploited, resulting in massive financial losses. The Decentralized Autonomous Organization (DAO) was vulnerable to ''reentrancy'' and the exploitation, detailed in [108], led to the loss of 3.6 million Ether. The authors in [109] propose a study of attacks on Ethereum smart contracts discovered before 2017. The authors in [110] present a framework for analyzing and verifying both runtime safety and functional correctness of Ethereum smart contracts. This framework allows the detection of ''reentrancy'' and ''exception confusion'' vulnerabilities. In [111], the authors propose Oyente, which is an execution tool made to detect vulnerabilities in Ethereum smart contracts and was able to detect an ''exception confusion'' vulnerability in 28% of the analyzed smart contracts. However, this framework proposed in [110] and this tool proposed in [111] are still immature because they cannot detect low-level vulnerabilities and only support Ethereum. They also need to be updated when new vulnerabilities are discovered. Currently, smart contracts do not have a mature regulatory framework [112].

VI. DISCUSSION ABOUT E-VOTING

A. EXPERIMENTS WITH E-VOTING

Before blockchain, e-voting already existed in Europe and around the world. Several e-voting systems, that do not use blockchain, have been introduced in Estonia, Switzerland and Norway [113]. In Estonia and Switzerland, e-voting has shown very satisfactory results, but in Norway it was abandoned in 2014 for security reasons and because e-voting did not substantially reduce the abstention rate. Nevertheless, in Estonia, in the last parliamentary elections of 2019, almost 44% of the votes were cast online, which is an unprecedented score, marking the success of this voting method among the population.

In any case, whether these experiments worked or not, they have allowed to test e-voting in real conditions on a national scale, which is not yet the case for blockchain. They have highlighted the possible flaws of such a system that are not tolerated for such issues. Moreover, it is important to specify that these implementations remain centralized and therefore subject to drawbacks that the blockchain allow to mitigate, thanks to its decentralized nature. But first, let's take a closer look at the considerations to have when judging the proper functioning of an e-voting application.

B. LEGAL AND POLITICAL CONSIDERATIONS FOR E-VOTING

Because of its institutional nature, e-voting must first be considered from a legal and political perspective [113].

1) LEGAL ASPECTS

The standards and regulations of the various countries define the criteria and prerequisites for voting, whether it is on paper or online. In the study [113], it is stated that any e-voting application must first comply with the fundamental principles enshrined in the law. Thus, a direct **vote must be universal, fair, free and, above all, secret**. Apart from the criterion of free voting, which does not seem to be particularly threatened by the e-vote [114], the other three must be taken into consideration. **Universal** suffrage means that all adult citizens are called to vote, and have the opportunity to do so. However, given the digital divide caused by the lack of basic computer skills and Internet connection problems of many people (elderly but not only), many citizens would be excluded from e-voting, which is not acceptable. Massive training of digitally challenged people should therefore be considered a prerequisite for e-voting, regardless of the technology chosen. We will come back to this point at the end of this paper. Concerning the **fairness** of the e-vote, i.e. that with a voter is associated a unique vote, it is also very difficult to ensure compared to the paper vote. Indeed, it is very difficult to verify perfectly the identity of the person who votes remotely. There is nothing to ensure that the person who votes is the person he claims to be. The question of the authentication system of the voter is thus essential, and we studied it more in detail in section IV. Finally, **confidentiality** is also one of the fundamental principles of voting guaranteed by law. This criterion depends considerably on the implementation and the quality of the e-voting system. **We will see how blockchain meets this constraint particularly well.** Even if an e-voting solution meets these expectations, the authors of the report [113] specify that an evolution of the regulatory framework of the countries wishing to set up an e-voting system will have to be conducted.

2) POLITICAL ASPECTS

The choice to implement e-voting has political consequences that cannot be excluded from the analysis. The **Trust** of all voters in the voting system is essential for the outcome of an election to be considered valid. The underlying question of the **transparency** of the voting system is therefore to be taken into account when choosing a voting technology. This transparency in paper voting is ensured by the physical counting of the ballots, controlled and assured by the citizens. Nevertheless, in non-democratic countries, this transparency criterion is undermined when the ballots are counted, hidden to the population. E-voting should therefore address this issue and allow citizens to see how votes are counted and how

the system works in general. This constraint also seems to be particularly well respected by e-voting via blockchain. One should not forget the **financial costs** of developing and implementing such a voting technology, as it involves public money. The cost-effectiveness balance must be carefully studied, so that the system is not doomed to failure in the long term. Finally, **the role of private companies** in the implementation of such a system is a major issue [100]. In the course of our analysis, we encountered a number of e-voting applications developed by private organizations that offer interesting innovations. But the interference of private companies in a public vote raises questions, both from an ethical and political perspective. Estonia has largely developed its own e-voting technologies, but more and more voting experiments have been conducted through a partnership between private companies and states. Blockchain relies primarily on private investment at the moment, so this question must be asked.

C. TECHNICAL CONSIDERATIONS FOR E-VOTING

Once the legal and political constraints have been established, we can now define the technical constraints that an e-voting application must respect [115]. These constraints can be divided into two main groups: those related to the human and those related to the technology.

- **Human-related constraints** may include the following:
  - Have an easy-to-use voting system: **usability**.
  - Guarantee citizens that their vote remains secret and that their identity cannot be traced from their vote: **privacy** and **confidentiality**.
  - Prove to citizens that the voting system is working properly (i.e., prove that votes are being counted and stored correctly): **transparency**, **audit** and **voter-verifiability**.
  - Prevent the intervention of an outsider to force another to vote in a certain way (i.e., prevent intimidation, fraud, forced vote selling, etc.): **resistance to coercion**. We note that this criterion is complicated to apply in the absence of a voting booth.
  - Do not discriminate against voters who cannot or will not have access to the Internet by offering an alternative to e-voting with their own devices: **eligibility**.
- **Technology-related constraints** may include the following:
  - Address the inequality of internet access opportunities between different socio-demographic groups. Some people who currently have poor internet connections need to be able to vote.
  - Prevent any attack, system failure or connection failure.
  - Consideration of the possible presence of viruses or malware on voters' personal computers that could (1) distort the voting decision and/or (2) affect the overall Internet voting system.
  - Ensure **voter authentication**.
  - Prevent multiple voting.

Among these constraints, the provision of broadband internet access for all, or the possibility of a paper alternative are not directly related to the voting application but to the public authority in charge of the election. However, compliance with all other criteria is primarily the responsibility of the e-voting application. Some e-voting applications seem to respect some of these constraints, as shown for example by the Estonian elections. The EU is also conducting pilot work in this direction in order to introduce a secure and reliable e-voting system [83]. In the course of this article, we see how the blockchain may, or may not, address these constraints more effectively than more traditionally used technologies for e-voting.

D. CASE STUDIES AND ONGOING RESEARCH PROJECTS

Although blockchain-based e-voting systems are still in their infancy (less than a decade old), several case studies have been reported on these systems. The case study presented in [116] shows how to digitize the European Election process by following a method designed and tested on the Ethereum blockchain. In another case study [117], the technology non profit Democracy Earth Foundation launched the e-voting platform to allow Colombians abroad to cast symbolic votes through the platform in the context of approving a peace treaty. The case study in [118] describes a blockchain-based mobile e-voting application that was deployed in 2018 in West Virginia for overseas military voters in the U.S. midterm elections, as well as for smaller-scale elections. A blockchain-based e-voting system was also used in Moscow, Russia, for the city council elections [119].

On the other hand, some research projects are ongoing to consider the use of blockchain for e-voting. For example, a system in Japan will be based on social security cards to verify the identity of voters and on blockchain to prevent the falsification of any registered data [120]. Currently, this system is being tested to cast votes on social contribution projects. Another project that is VotingDAO which brings a fully decentralized e-voting system to the blockchain, where the system will be governed by a smart contract to ensure its transparency, reliability and accountability [121]. Moreover, companies like Voatz and Follow My Vote are using blockchain technology to create a new e-voting system. It is worth noting that some accredited international observers have used blockchain to ensure that election data is third-party verifiable and protected against the possibility of tampering [122].

VII. CONCLUSION

Blockchain appears as an interesting alternative to traditional voting systems. The world of blockchain is a constantly evolving ecosystem, as many are created while others disappear. Indeed, in the scientific literature, more and more research works propose e-voting applications based on blockchain. Nevertheless, only a few of the proposed solutions have been implemented in real life and none have been tested on a large scale. Therefore, it is very difficult to con-

clude that blockchain is a fully secure alternative to conduct a national election nowadays. Although the principles on which blockchain is based are secure, e-voting applications are still vulnerable to several attacks. This makes it very challenging to guarantee the integrity of an election, which is problematic given the stakes of such an application.

Moreover, it is important to note that blockchain does not eliminate the need for a central authority to organize an election. Any organization of a country-wide election necessarily implies a minimal amount of centralization, mainly to produce the list of eligible voters. However, there are other avenues that can be explored for the use of blockchain in future elections. While the use of blockchain alone to organize a vote seems unrealistic now, it is possible to consider its use as a complement to current systems. For example, one could imagine using a blockchain to count paper votes at the level of each municipality or region, thereby reducing the risk of fraud and lack of trust. Furthermore, in countries with large territories, a voting application using blockchain on smartphones (in addition to physical polling stations) would allow a greater participation of people initially excluded from the democratic process due to their geographical isolation.

REFERENCES

[1] M. J. Beck and D. A. Hensher, "Insights into the impact of COVID-19 on household travel and activities in Australia—The early days under restrictions," *Transp. Policy*, vol. 96, pp. 76–93, Sep. 2020.

[2] D. Duenas-Cid, I. Krivonosova, R. Serrano, M. Freire, and R. Krimmer, "Tripped at the finishing line: The Åland islands internet voting project," in *Proc. Int. Joint Conf. Electron. Voting*. Cham, Switzerland: Springer, 2020, pp. 36–49.

[3] R. Krimmer, D. Duenas-Cid, and I. Krivonosova, "New methodology for calculating cost-efficiency of different ways of voting: Is internet voting cheaper?" *Public Money Manage.*, vol. 41, no. 1, pp. 1–10, 2020.

[4] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: From internet voting to blockchain voting," *J. Cybersecurity*, vol. 7, no. 1, pp. 1–15, Feb. 2021.

[5] N. El Madhoun, J. Hatin, and E. Bertin, "A decision tree for building IT applications," *Ann. Telecommun.*, vol. 76, nos. 3–4, pp. 131–144, Apr. 2021.

[6] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri, and S. Gupta, "A comparitive analysis on E-voting system using blockchain," in *Proc. 4th Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Apr. 2019, pp. 1–4.

[7] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, no. 8, p. 1328, Aug. 2020.

[8] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. Electron. Workshops Comput.*, Jun. 2008, pp. 1–10.

[9] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, "E-voting systems using blockchain: An exploratory literature survey," in *Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2020, pp. 890–895.

[10] M. Pawlak and A. Poniszewska-Marańda, "Trends in blockchain-based electronic voting systems," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102595.

[11] D. Maldonado-Ruiz, J. Torres, N. El Madhoun, and M. Badra, "An innovative and decentralized identity framework based on blockchain technology," in *Proc. 11th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Apr. 2021, pp. 1–8.

[12] J. Hatin, E. Bertin, B. Hemery, and N. E. Madhoun, "Welcome to the jungle: A reference model for blockchain, DLT and smart-contracts (short paper)," in *Proc. 2nd Int. Conf. Blockchain Econ., Secur. Protocols*, 2021, pp. 1–6.

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[14] M. D. Chiesa, F. Hiault, and C. Téqui, "Blockchain: Vers de nouvelles chaînes de valeur," *Eyrolles*, 2019.

[15] N. Szabo, "Formalizing and securing relationships on public networks," *1st Monday*, vol. 2, no. 9, Sep. 1997.

[16] V. Buterin, "Ethereum white paper: A next generation smart contract & decentralized application platform," White Paper, 2013, vol. 3, no. 37.

[17] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2018, pp. 1–6.

[18] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020.

[19] J.-H. Hsiao, R. Tso, C.-M. Chen, and M.-E. Wu, "Decentralized E-voting systems based on the blockchain technology," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2017, pp. 305–309.

[20] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," *Future Gener. Comput. Syst.*, vol. 112, pp. 859–874, Nov. 2020.

[21] M. Chaieb and S. Yousfi, "Loki vote: A blockchain-based coercion resistant E-voting protocol," in *Proc. Eur., Medit., Middle Eastern Conf. Inf. Syst.* Cham, Switzerland: Springer, 2020, pp. 151–168.

[22] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on ethereum blockchain," in *Proc. IEEE Int. Multidisciplinary Conf. Eng. Technol. (IMCET)*, Nov. 2018, pp. 1–6.

[23] R. Hanifatunnisa and B. Rahardjo, "Blockchain based E-voting recording system design," in *Proc. 11th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2017, pp. 1–6.

[24] H. Yi, "Securing E-voting based on blockchain in P2P network," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–9, Dec. 2019.

[25] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 401–408.

[26] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, "E-voting with blockchain: An E-voting protocol with decentralisation and voter privacy," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1561–1567.

[27] F. P. Hjálmarsson, G. K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based E-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 983–986.

[28] A. M. Larriba, A. C. I. Cucó, J. M. Sempere, and A. López, "Distributed trust, a blockchain election scheme," *Informatica*, vol. 32, no. 2, pp. 1–35, 2021.

[29] G. Srivastava, A. D. Dwivedi, and R. Singh, "Crypto-democracy: A decentralized voting scheme using blockchain technology," *ICETE*, vol. 2, pp. 674–679, Jul. 2018.

[30] P. Emerson, "The original Borda count and partial voting," *Social Choice Welfare*, vol. 40, no. 2, pp. 353–358, 2013.

[31] K. Sadia, M. Masuduzzaman, R. K. Paul, and A. Islam, "Blockchain-based secure E-voting with the assistance of smart contract," in *IC-BCT*. Singapore: Springer, 2020, pp. 161–176.

[32] E. Danso, J. Appiah, and B. Odoi-Lartey, "Digital voting systems deploying the use of blockchain technology," *Int. J. Comput. Appl.*, vol. 178, no. 53, pp. 1–4, Sep. 2019.

[33] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for board room voting with maximum voter privacy," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2017, pp. 357–375.

[34] A. S. Yadav, A. U. Thombare, Y. V. Urade, and A. A. Patil, "E-voting using blockchain technology," *Int. J. Eng. Res. Technol.*, vol. 9, no. 7, 2020.

[35] S. Shukla, A. N. Thasmiya, D. O. Shashank, and H. R. Mamatha, "Online voting application using ethereum blockchain," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 873–880.

[36] A. M. Al-madani, A. T. Gaikwad, V. Mahale, and Z. A. T. Ahmed, "Decentralized E-voting system based on smart contract by using blockchain technology," in *Proc. Int. Conf. Smart Innov. Design, Environ., Manage., Planning Comput. (ICSIDEMPC)*, Oct. 2020, pp. 176–180.

[37] R. L. Almeida, L. Ricci, and L. M. Camarinha-Matos, "VoteChain: Community based scalable internet voting framework," in *Proc. Doctoral Conf. Comput., Elect. Ind. Syst.* Cham, Switzerland: Springer, 2019, pp. 70–80.

[38] D. MohanaPriya, G. Devadharshini, S. Divya, and J. Rajalatchumy, "Towards a privacy-preserving voting system through blockchain technologies," in *Proc. Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN)*, Jul. 2021, pp. 602–608.

[39] C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, and L. Mauri, "Towards blockchain-based E-voting systems," in *Proc. Int. Conf. Bus. Inf. Syst.* Cham, Switzerland: Springer, 2019, pp. 274–286.

[40] M. Chaieb, S. Yousfi, P. Lafourcade, and R. Robbana, "Verify-your-vote: A verifiable blockchain-based online voting protocol," in *Proc. Eur., Medit., Middle Eastern Conf. Inf. Syst.* Cham, Switzerland: Springer, 2018, pp. 16–30.

[41] C. Killer, B. Rodrigues, E. J. Scheid, M. Franco, M. Eck, N. Zaugg, A. Scheitlin, and B. Stiller, "Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 172–183.

[42] R. Krishnamurthy, G. Rathee, and N. Jaglan, "An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices," *Wireless Netw.*, vol. 26, no. 4, pp. 2391–2402, May 2020.

[43] H. Li, Y. Li, Y. Yu, B. Wang, and K. Chen, "A blockchain-based traceable self-tallying E-voting protocol in AI era," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1019–1032, Apr. 2021.

[44] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless E-Voting system based on smart contract," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 570–577.

[45] S. Panja, S. Bag, F. Hao, and B. Roy, "A smart contract system for decentralized Borda count voting," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1323–1339, Nov. 2020.

[46] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure online voting system using biometric and blockchain," in *Data Management, Analytics and Innovation*. Singapore: Springer, 2020, pp. 93–110.

[47] A. J. Perez and E. N. Ceesay, "Improving end-to-end verifiable voting systems with blockchain technologies," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1108–1115.

[48] K. L. S. Priya and C. Rupa, "Block chain technology based electoral franchise," in *Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 1–5.

[49] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, "AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102069.

[50] L. Vo-Cao-Thuy, K. Cao-Minh, C. Dang-Le-Bao, and T. A. Nguyen, "Votereum: An ethereum-based E-voting system," in *Proc. IEEE-RIVF Int. Conf. Comput. Commun. Technol. (RIVF)*, Mar. 2019, pp. 1–6.

[51] Z. Xu and S. Cao, "Efficient privacy-preserving electronic voting scheme based on blockchain," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2020, pp. 190–196.

[52] Y. Zhang, Y. Li, L. Fang, P. Chen, and X. Dong, "Privacy-protected electronic voting system based on blockchin and trusted execution environment," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2019, pp. 1252–1257.

[53] B. Yu, J. K. Liu, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, and A. H. Au, "Platform-independent secure blockchain-based voting system," in *Proc. Int. Conf. Inf. Secur.* Cham, Switzerland: Springer, 2018, pp. 369–386.

[54] E. Bellini, P. Ceravolo, A. Bellini, and E. Damiani, "Designing process-centric blockchain-based architectures: A case study in E-voting as a service," in *Data-Driven Process Discovery and Analysis*. Cham, Switzerland: Springer, 2018, pp. 1–23.

[55] S. Chaisawat and C. Vorakulpipat, "Fault-tolerant architecture design for blockchain-based electronics voting system," in *Proc. 17th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, Nov. 2020, pp. 116–121.

[56] X. Jiang, M. Liu, F. Zhao, Q. Zhou, and R. Wang, "Fast adaptive blockchain's consensus algorithm via WLAN mesh network," in *Proc. Int. Conf. Secur. Intell. Comput. Big-Data Services*. Cham, Switzerland: Springer, 2018, pp. 3–16.

[57] D. Kirillov, V. Korkhov, V. Petrunin, M. Makarov, I. M. Khamitov, and V. Dostov, "Implementation of an E-voting scheme using hyperledger fabric permissioned blockchain," in *Proc. Int. Conf. Comput. Sci. Appl.* Cham, Switzerland: Springer, 2019, pp. 509–521.

[58] P. Li and J. Lai, "LaT-Voting: Traceable anonymous E-voting on blockchain," in *Proc. Int. Conf. Netw. Syst. Secur.* Cham, Switzerland: Springer, 2019, pp. 234–254.

[59] D. Seftyanto, A. Amiruddin, and A. R. Hakim, "Design of blockchain-based electronic election system using hyperledger: Case of Indonesia," in *Proc. 4th Int. Conf. Inf. Technol., Inf. Syst. Electr. Eng. (ICITISEE)*, Nov. 2019, pp. 228–233.

[60] M. Soud, S. Helgason, G. Hjalmtysson, and M. Hamdaqa, "TrustVote: On elections we trust with distributed ledgers and smart contracts," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 176–183.

[61] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: Secret SHARe-based VOTing on the blockchain," in *Proc. 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain*, May 2018, pp. 30–34.

[62] Z. Zhao and T. H. H. Chan, "How to vote privately using bitcoin," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2015, pp. 82–96.

[63] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *Int. J. Netw. Secur. Appl.*, vol. 9, no. 3, pp. 1–9, 2017.

[64] H. V. Patil, K. G. Rathi, and M. V. Tribhuwan, "A study on decentralized e-voting system using blockchain technology," *Int. Res. J. Eng. Technol*, vol. 5, no. 11, pp. 48–53, 2018.

[65] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access* vol. 7, pp. 24477–24488, 2019.

[66] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *Int. J. Electron. Government Res.*, vol. 14, no. 1, pp. 53–62, Jan. 2018.

[67] T. M. Roopak and R. Sumathi, "Electronic voting based on virtual ID of aadhar using blockchain technology," in *Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 71–75.

[68] Agora. (2017). *Agora: Bringing Our Voting Systems Into the 21st Century*. [Online]. Available: https://www.agora.vote/resources

[69] R. Taş and Ö. Ö. Tanrıöver, "A manipulation prevention model for blockchain-based E-voting systems," *Secur. Commun. Netw.*, vol. 2021, pp. 1–16, Apr. 2021.

[70] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, X. Du, and M. Guizani, "A blockchain-based self-tallying voting protocol in decentralized IoT," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 119–130, Jan. 2022.

[71] J. C. Priya, P. R. K. S. Bhama, S. Swarnalaxmi, A. A. Safa, and I. Elakkiya, "Blockchain centeblack homomorphic encryption: A secure solution for E-balloting," in *Proc. Int. Conf. Comput. Netw., Big Data IoT*. Cham, Switzerland: Springer, 2018, pp. 811–819.

[72] E. Zaghloul, T. Li, and J. Ren, "Anonymous and coercion-resistant distributed electronic voting," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2020, pp. 389–393.

[73] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: Blockchain-enabled large-scale E-voting system with robustness and universal verifiability," *Int. J. Inf. Secur.*, vol. 19, no. 3, pp. 323–341, Jun. 2020.

[74] T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," *Comput. Netw.*, vol. 174, Jun. 2020, Art. no. 107234.

[75] Y. Liu and Q. Wang, "An E-voting protocol based on blockchain," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 1043, Oct. 2017.

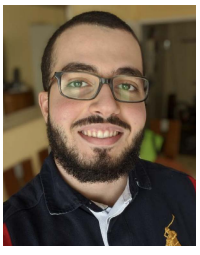
[76] Y. Wu, "An E-voting system based on blockchain and ring signature," *Master. Univ. Birmingham*, 2017.

[77] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based E-voting system using biohash and smart contract," in *Proc. 3rd Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Aug. 2020, pp. 228–233.

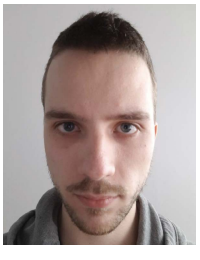
[78] M. Chaieb, M. Koscina, S. Yousfi, P. Lafourcade, and R. Robbana, "Dabsters: A privacy preserving E-voting protocol for permissioned blockchain," in *Proc. Int. Colloq. Theor. Aspects Comput.* Cham, Switzerland: Springer, 2019, pp. 292–312.

[79] G. Han, Y. Li, Y. Yu, K.-K.-R. Choo, and N. Guizani, "Blockchain-based self-tallying voting system with software updates in decentralized IoT," *IEEE Netw.*, vol. 34, no. 4, pp. 166–172, Jul. 2020.

[80] Y. Zhou, Y. Liu, C. Jiang, and S. Wang, "An improved FOO voting scheme using blockchain," *Int. J. Inf. Secur.*, vol. 19, no. 3, pp. 303–310, Jun. 2020.
[81] R. A. Mollin, *RSA and Public-Key Cryptography*. Boca Raton, FL, USA: CRC Press, 2002.
[82] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," *Int. J. U e-Service, Sci. Technol.*, vol. 2, no. 3, pp. 13–28, 2009.
[83] D. Hühnlein. (2021). *Mobile Cross-Border Government Services for Europe*. (Nov. 10, 2021). [Online]. Available: https://www.mgov4.eu/fileadmin/mgov-files/pub/mGov4EU-D1.3-PU-M06.pdf
[84] R. Ganji and B. Yatish, "Electronic voting system using blockchain," Dell EMC, Round Rock, TX, USA, Tech. Rep., 2018.
[85] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS)*, Oct. 2018, pp. 22–27.
[86] G. Srivastava, A. D. Dwivedi, R. Singh, and R. Singh, "Phantom protocol as the new crypto-democracy," in *Proc. IFIP Int. Conf. Comput. Inf. Syst. Ind. Manage.* Cham, Switzerland: Springer, 2018, pp. 499–509.
[87] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting, a blockchain based E-voting system," in *Proc. KMIS*, 2018, pp. 221–225.
[88] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Proc. Int. Workshop Sel. Areas Cryptography*. Berlin, Germany: Springer, 2003, pp. 175–193.
[89] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2002, pp. 533–547.
[90] M. Rockwell. (2014). *Bitcongress*. (Dec. 23, 2021). [Online]. Available: https://www.bitcongress.org/
[91] (2015). *Follow My Vote*. (Dec. 23, 2021). [Online]. Available: https://followmyvote.com/
[92] Smartmatic. (Dec. 23, 2021). *TIVI*. [Online]. Available: https://www.smartmatic.com/elections/remote-voting/tivi/
[93] N. Faour, "Transparent E-voting dApp based on waves blockchain and RIDE language," in *Proc. 16th Int. Symp. Problems Redundancy Inf. Control Syst. (REDUNDANCY)*, Oct. 2019, pp. 219–223.
[94] S. H. Shaheen, M. Yousaf, and M. Jalil, "Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain," in *Proc. 13th Int. Conf. Emerg. Technol. (ICET)*, Dec. 2017, pp. 1–6.
[95] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain," *Int. J. Theor. Phys.*, vol. 58, no. 1, pp. 275–281, Jan. 2019.
[96] M. B. Verwer, I. Dionysiou, and H. Gjermundrød, "Trustedevoting (TeV) a secure, anonymous and verifiable blockchain-based e-voting framework," in *Proc. Int. Conf. e-Democracy*. Cham, Switzerland: Springer, 2019, pp. 129–143.
[97] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, "E-voting system using hyperledger sawtooth," in *Proc. Int. Conf. Adv. Comput., Commun. Mater. (ICACCM)*, Aug. 2020, pp. 29–35.
[98] A. A. Leema, Z. Gulzar, and P. Padmavathy, "Trusted and secublack E-voting election system based on block chain technology," in *Proc. Int. Conf. Comput. Netw., Big Data IoT*. Cham, Switzerland: Springer, 2019, pp. 81–88.
[99] V. Cortier, A. Debant, and P. Gaudry, "A privacy attack on the Swiss post E-voting system," Ph.D. thesis, Université de Lorraine, CNRS, Inria, LORIA, Nancy, France, 2021.
[100] A. Juels, I. Eyal, and O. Naor. (2018). *Blockchain Won't Fix Internet Voting Security- and Could Make it Worse*. (Jan. 15, 2022). [Online]. Available: https://theconversation.com/blockchains-wont-fix-internet-voting-security-and-could-make-it-worse-104830
[101] R. Goodman and J. A. Halderman. (2020). *Internet Voting is Happening Now*. (Jan. 15, 2022). [Online]. Available: https://slate.com/technology/2020/01/internet-voting-could-destroy-our-elections.html
[102] *Securing the Vote: Protecting American Democracy*, Nat. Academies Sci., Eng., Med., 2018.
[103] A. M. Specter, J. Koppel, and D. Weitzner, "The ballot is busted before the blockchain: A security analysis of Voatz, the first internet voting application used in U.S. Federal elections," in *Proc. 29th USENIX Secur. Symp. (USENIX Security)*, 2020, pp. 1535–1553.
[104] N. Kshetri and J. Voas, "Blockchain-enabled E-voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.
[105] P. Norris, *The Digital Divide*. Evanston, IL, USA: Routledge, 2020.
[106] I. Abraham, G. Gueta, D. Malkhi, L. Alvisi, R. Kotla, and J.-P. Martin, "Revisiting fast practical byzantine fault tolerance," 2017, *arXiv:1712.01367*.
[107] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," 2017, *arXiv:1707.01873*.
[108] P. Daian. (2016). *Analysis of the DAO Exploit*. [Online]. Available: https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/
[109] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Proc. Int. Conf. Princ. Secur. Trust*. Berlin, Germany: Springer, 2017, pp. 164–186.
[110] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Zanella-Béguelin, "Formal verification of smart contracts: Short paper," in *Proc. ACM Workshop Program. Lang. Anal. Secur.*, 2016, pp. 91–96.
[111] S. Badruddoja, R. Dantu, Y. He, K. Upadhayay, and M. Thompson, "Making smart contracts smarter," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 254–269.
[112] J. Ellul, J. Galea, M. Ganado, S. Mccarthy, and G. J. Pace, "Regulating blockchain, DLT and smart contracts: A technology regulator's perspective," *ERA Forum*, vol. 21, no. 2, pp. 209–220, Oct. 2020.
[113] A. Trechsel. (2016). *Potential and Challenges of E-Voting in the European Union*. (Nov. 10, 2021). [Online]. Available: https://cadmus.eui.eu/bitstream/handle/1814/44926/EUDO_REPORT_2016_11.pdf?sequence=1
[114] P. Garrone, *Fundamental and Political Rights in Electronic Elections*. Evanston, IL, USA: Routledge, 2004.
[115] M. Bernhard, J. Benaloh, J. A. Halderman, R. L. Rivest, P. Y. A. Ryan, P. B. Stark, V. Teague, P. L. Vora, and D. S. Wallach, "Public evidence from secret ballots," in *Proc. Int. Joint Conf. Electron. Voting*. Cham, Switzerland: Springer, 2017, pp. 84–109.
[116] M. Skotnica, M. Aparício, R. Pergl, and S. Guerreiro, "Process digitalization using blockchain: EU parliament elections case study," in *Proc. MODELSWARD*, 2021, pp. 65–75.
[117] *Embracing Innovation in Government—Blockchain Voting for Peace in Colombia*. (Dec. 23, 2021). [Online]. Available: https://www.oecd.org/gov/innovative-government/embracing-innovation-in-government-colombia.pdf
[118] *West Virginia Secretary of State's Office. 24 Counties to Offer Mobile Voting Option for Military Personnel Overseas*. (Dec. 23, 2021). [Online]. Available: https://sos.wv.gov/news/Pages/09-20-2018-A.aspx
[119] *Official Website of the Mayor of Moscow*. (Dec. 23, 2021). [Online]. Available: https://www.mos.ru/news/item/58866073
[120] C. Osborne. (2018). *Japanese City Trials Blockchain to Replace Traditional Voting Booths*. (Dec. 23, 2021). [Online]. Available: https://thenextweb.com/news/japan-city-blockchain-voting
[121] (2022). *VotingDAO Announces Upcoming Inaugural Blockchain Person of the Year Decentralized Voting Event*. (Jan. 15, 2022). [Online]. Available: https://zycrypto.com/votingdao-announces-upcoming-inaugural-blockchain-person-of-the-year-decentralized-voting-event/
[122] (2018). *Swiss-Based Agora Records First Government Election on Blockchain as Accblackited Observer in Sierra Leone*. (Jan. 15, 2022). [Online]. Available: https://medium.com/agorablockchain/swiss-based-agora-powers-worlds-first-ever-blockchain-elections-in-sierra-leone-984dd07a58ee



ALI BENABDALLAH is currently pursuing the master's degree with the École Polytechnique Fédérale de Lausanne (EPFL), Switzerland. In 2021, he obtained a computer science license from Sorbonne Université, Paris. His research interests include blockchain, smart-contracts, and machine learning.



ANTOINE AUDRAS is currently pursuing the master's degree in données apprentissage connaissances (DAC) with Sorbonne Université. He has obtained a computer science license from Sorbonne Université, in 2021. His research interests include blockchain and smart-contracts technologies, deep learning, continual learning, and natural language processing.

LOUIS COUDERT received the dual bachelor's degree in computer science and political science from Sorbonne Université and Sciences Po Paris, in 2021. He is currently pursuing the master's degree in public policies with Sciences Po Paris. His research interests include cybersecurity issues, especially in the protection of public administrations, blockchain, and smart-contracts technologies.

NOUR EL MADHOUN received the master's degree in networks/computer science from Sorbonne Université/Télécom ParisTech, in 2014, and the Ph.D. degree in cybersecurity/computer science from Sorbonne Université, in 2018. In 2018, she gained industry experience through working as a Postdoctoral Researcher at Orange Labs.

At Sorbonne Université, she became an ATER, in 2017. In 2019, she joined ISEP—an engineering school, Paris, as an Associate Professor of cybersecurity in addition to overseeing the engineering cycle—digital security and networks. From 2020 to 2022, she joined EPITA—an engineering school, Paris, as an Associate Professor of cybersecurity and blockchain. She is currently an Associate Professor of computer science, cybersecurity and blockchain at ISEP—an engineering school, Paris. She is also an Associate Researcher at Sorbonne Université (LIP6-PHARE Team). Her current research interests include network security, cryptographic protocols, EMV payment, NFC technology, blockchain, and smart-contracts technologies.

MOHAMAD BADRA received the Ph.D. degree in security and networking from Télécom ParisTech (ex. ENST). He is currently an Associate Professor at Zayed University. He is the author of several international standards on security exchange and the coauthor of many international conference and journal papers. His research interests include information security, smart city (smart grid and urban sensing), wireless sensor networks, with a focus on designing, building, analyzing, and measuring privacy and security protocols, and secure architectures for wired/wireless networks.