Review on Blockchain based e-Voting Systems

Nomana Ayesha Majeed
Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida

With the advancement in cryptography and emerging internet technology, electronic voting is gaining popularity since it ensures ballot secrecy, voter security, and integrity. Many commercial startups and e-Voting systems have been proposed, but due to lack of trust, privacy, transparency, and hacking issues, many solutions have been suspended. Blockchain, along with cryptographic primitives, has emerged as a promising solution due to its transparent, immutable, and decentralized nature. In this paper, we summarized the properties that existing solutions should satisfy and explained some cryptographic primitives like ZKP, Ring signatures along with their security limitations. We gave a comprehensive review of some block-chain-based e-Voting systems and discussed their strengths and weaknesses based on the given properties with table of comparison.

1. Introduction

Elections are the cornerstone of leadership selection in any democratic country. For many years, paper-based voting systems have been used for important decisions. This method has many risks related to privacy disclosure, insecurity, and biased voting.

Since 1980, many e-Voting systems have attracted the researchers around the world [22] like in Estonia [40], USA, Australia, and Switzerland to solve the problems faced by traditional voting systems. E-Voting aims to improve security, efficiency, cost-efficiency. Meanwhile, many challenges have been identified in such systems such as corrupt administration, trust in central party, lack of efficient software, secrecy of ballots [41].

Trust is the most complex problem in e-Voting, and blockchain [23] has emerged as a solution to many of the aforementioned problems. In 2009, Nakamoto [21] introduced the blockchain which was preliminary used for cryptocurrencies [31] but now it has become a core component in various other areas of identification, authorization including the smart contracts [30], particularly in e-Voting to solve the issue of trust in the central party. Blockchain is mainly deployed in three forms: smart contract-based e-Voting [3], cryptocurrency-based e-Voting, and as a ballot box [7]. So far, many researched based and commercial-scale voting systems have been deployed, such as Agora [2], Voatz [42], FMV [7].

The rest of the paper is organized as follows: In Section II, we describe the properties that serve as criteria for recently proposed blockchain-based e-voting solutions. In Section III, we discuss ZKP, ring signatures, blind signatures and some other traditional cryptographic algorithms, and their limitations. In section IV, we present a comprehensive review of some blockchain-based e-Voting systems and discuss their strengths and weaknesses based on the given properties. Finally, we illustrate a table ii comparing e-Voting protocol and highlight the areas where improvements can be made.

2. Properties of a robust e-Voting system

We considered thirteen security properties collected from various experimented blockchain-based electronic voting systems. The definitions vary from paper to paper according to their requirements, we provide a refined description of the properties that can serve as an evaluation-criteria for existing protocols.

P1. Privacy: the relationship between the vote and voter should not be revealed and vote must be kept secret.

P2. Anonymity: the protocol should protect the voter´s anonymity while casting the vote.

P3. Robustness: protocol should be capable of tolerating a certain amount of technical failure and participant misbehavior.

P4. Eligibility verification: only registered and authorized voters can participate.

P5. Individual verifiability (E2E): a voter can verify that his vote was casted-as-intended, recorded-as-casted and counted-as-recorded.

P6. Universal verifiability: anyone can download the tallied result, and check the completeness of elections.

P7. Scalability: the e-Voting system should be capable of supporting large-scale elections.

P8. Fairness: protocol should not be capable of providing any partial results before the tallying phase.

P9. Receipt-freeness [19]***:*** the voting system should not generate any receipt to prove whom the voter has voted for. Consequently, a voter cannot provide any proof to third party, this stops vote-buying and selling.

P10. Untraceability [24]***:*** the voter and third party should not be able to trace the vote back to him even after decryption of results.

P11. Coercion resistance *(vote-freely)* [20]***:*** it is the strongest notion of privacy where no voter can prove that he followed the coercer´s instructions. It ensures receipt-freeness but it requires an anonymous channel.

P12. Un-reusability: one vote per eligible voter, it prevents replay attack.

P13. Vote-and-go: a voter can go after casting his ballot.

Furthermore, individual verifiability and receipt-freeness are related. To achieve both properties together, it is required to generate proof that is sufficient for a voter to get verification but insufficient for a coercer to know how the voter has voted. Additionally, verifiability requires linkability and anonymity requires unlinkability of the voter. The voter should know that his vote is included in the tally but he cannot provide a prove for his vote since the vote is not unique [29]. Besides these properties, we have also evaluated the blockchain based e-Voting systems according to the platform, decentralization, voting choice, vote encryption, and cryptographic primitive being used.

Abbreviation	Explanation
ZKP	Zero Knowledge Proof
QAP	Quadratic Arithmetic Program
Zk-SNARKs	Zero knowledge Succinct Non-Interactive Argument of Knowledge
CRS	Common Reference String
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
LRS	Linkable Ring Signature
MAST	Merkelized Abstract Syntax Trees
MPC	Multi Party Computation

Table i: list of Abbreviations

3. Blockchain & Cryptography

3.1. Fundamentals of Blockchain

Blockchain [23] is a decentralized append-only ledger formed by chaining the blocks together. Each connected node has a backup of the entire database, so if someone tries to alter the transaction, it will be immediately detected by all other nodes. Blockchain has become a robust solution for both traditional and e-Voting system due to its characteristics namely: transparency, immutability and decentralization.
Although the blockchain has solved many challenges related to security, such as avoiding the manipulation of votes, fast and transparent voting results without third-party involvement, it is also important to highlight that existing blockchain based solutions have scalability issues, as each transaction need to be verified by the entire network, which reduces speed and increases cost. Moreover, due to the complexity of the computational steps, blockchain requires powerful systems to manage traffic in large elections. Secondly, blockchain is transparent by nature which we don't need in e-Voting systems. Instead, we need privacy and anonymity, and to this end, several traditional cryptographic techniques have been applied to ensure privacy. We have studied most commonly used cryptographic primitives in e-Voting systems and highlighted the limitations. These includes zero knowledge proofs, zk-SNARKs, ring signatures, blind signatures, homomorphic encryption, mix-networks, secret sharing scheme and elliptic curve cryptography [27] [34] [37].

3.2. Zero knowledge proof

ZKP is a cryptographic method invented by [25] in which a prover can prove to the verifier that he knows a certain statement without revealing any information about the statement except the truth. ZKP must satisfy the three properties, namely: completeness, reliability, and zero knowledge. In an e-Voting system, Non-Interactive ZKP is widely used [14], and is obtained by applying the Fiat-Shamir heuristic to prove the validity of a ciphertext, i.e., the voter convinces the third party that his ballot is valid by proving a ZKP without revealing any information about the voter's choice.

The most commonly used ZKPs in electronic voting systems are Schnorr ZKP and zk-SNARKs [32]. zk-SNARKs are very complex proofs and require strong computational power in proofs generation since the arguments are used to prove an NP statement about a QAP without revealing anything about the witness. The main limitation in zk-SNARKs is the generation of CRS which requires the participation of multiple parties, if the parties are compromised then the entire voting system is destroyed. Secondly, ZKP rely on the hardness of the DLOG problem, which is challenging in long run, since as Shor [38] proved that the DLOG can be computed efficiently by quantum computers [12] [16].

3.3. Elliptic curve cryptography

Several digital signatures based on finite fields have been used in e-voting systems for authentication purpose. The recent focus of DSS is on elliptic curve like Schnorr DSS [39]. ECC [34] is an approach to asymmetric cryptography constructed on the algebraic structure of elliptic curves to provide high data security with smaller bit size than RSA. ECC uses elliptic curve point addition and multiplication to generate the keys that acts like a trapdoor. Thus, the difficulty lies in the infeasibility to compute the EC-DLOG problem. Despite the security of EC, side-channel attacks [33] and twist-security attacks make EC unsecure for e-Voting systems as they can overturn the security that ECC aims to provide. Side-channel attacks are more common in the practical implementation of a cryptosystem which often results in leakage of data, thus compromising confidentiality and anonymity.

3.4. Blind Signatures

Blind signature [36] allows a user to select a message, encrypt it and asks and the signer to signs the encrypted message. Hence, it is not the user that is blind but the signer due to the blindness factor involved in encryption! Such signatures are used when the user's privacy is particularly important. Therefore, these signatures are applied extensively in the e-Voting systems that allow an authority to verify the voter's identity. After receiving confirmation, the voter unblinds his encrypted vote and submits it to the tallying authority using an anonymous channel. Thus, ensures eligibility verification.

Although, such signatures are very simple, efficient, but due to the unlinkability of unblinded signature to the voter, it is difficult to find whether the voter cast multiple votes. Furthermore, such systems do not achieve receipt-freeness, since the voter can use the blind factors to link with his ballot to prove later how he voted. On the other hand, the coercer can dictate the voter to use the particular factor to blind his ballot that violates coercion resistance. Lastly, both the voter and the tallying authority must trust the signer. If the signing authority is compromised or refuses to sign, the voting system can stop working [6] [5] [14].

3.5. Ring Signatures

Ring signatures were introduced by [27] in a paper titled "how to leak a secret". It is an anonymized variant of the digital signature and does not require a trusted third party. Ring signatures are constructed in such a way that the ring can only be completed and correctly verified if the signer knows a secret for one of the given public keys in the ring. In e-Voting, the most frequently used ring signatures are linkable ring signatures, [26] where the identity of the signer remains anonymous but with an additional tag that provides linkability feature in case of double submission. The voter generates an LRS to cast his vote which provides anonymity to the vote while linkability helps to detect duplicate voting [9] [15]. Thus, three main advantages of LRS are anonymity, efficiency, and linkability. Many recent developments in e-Voting have used ring signatures [Monero] however, the size of the signature, cost, and time grow linearly with the number of users in many proposed e-Voting systems [11] since the ring contains all public keys that increases automatically with the number of voters, so it should be split into subgroups by using the "image of secret key".

3.6. Secret Sharing Scheme (SSS)

SSS [37] is a method that securely distributes the shares of a secret among a group of participants. Most e-Voting systems used Shamir secret sharing scheme (SSSS); a threshold scheme that uses polynomial interpolation. SSSS first encodes the "secret" into a "polynomial" then divides it into pieces and distributes it. To reconstruct the secret, we need atleast $t\,(threshold)+1$ participants. SSSS is typically used in e-Voting protocols to achieve robustness against corrupted authorities. [5] utilized SSSS to distribute the keys however, the scheme must trust a single dealer for the distribution of the shares. Though, some attacks are possible when shares are revealed asynchronously as long as there is an internal adversary or group of internal adversaries [28].

3.7. Mix-Networks

Mix-nets [35] are mainly used to ensure user anonymity. It consists of a set of mix servers that take encrypted data (votes) as input, re-encrypt it, mix it and pass the output to the next server. The process continues until the last server is reached. In this method, the input (identity of voter) and the final output (vote) remain completely unlinked, providing anonymity to the user. In practice, re-encryption mix-net is commonly used in e-Voting systems compared to decryption mix-net. ZKP is required to verify the honesty of each server which increases the computational complexity. Although, mix-net provide receipt freeness but such systems are less efficient due to the involvement of multiple intermediate steps and exposed to DDoS attacks since all mixers are required during the tally.

3.8. Homomorphic encryption (HE)

Homomorphic Encryption allows to operate on encrypted data without decrypting any information. In practice, additive homomorphic ElGamal encryption [2] [12] and multiplicative homomorphic Paillier encryption [6][8] are mostly used. In e-Voting schemes, the calculation is performed on the ciphertext, so each voter must generate a ZKP to provide the validity of the encrypted ballot. This provides universal verifiability, robustness, and privacy at the same time. However, a threshold of trustworthy tallying authorities is required to decrypt the election result. Such protocols do not require any anonymous channel, but complex strategies and slow computation time makes it inapplicable for large-scale elections. Also, both ElGamal and Paillier cryptosystems are subject to quantum attack.

4. Review of Blockchain based e-Voting systems

4.1. How to vote privately using Bitcoin [1]

Zhao and Chain (2015) proposed an e-Voting system based on Bitcoin using a threshold signature scheme and ZKP. The ballots do not need to be encrypted or decrypted instead random numbers are used to hide the ballot, which are distributed via ZKP. Each voter can fund exactly one of the two candidates, the candidate who is funded more wins the elections. Voting is done via two methods: Claim-or-Refund and Joint transaction. In Claim-or-Refund, if a voter does not reveal his masked vote, all 2n COR instances will expired and the protocol is terminated. In joint transaction, all transactions remain secret and any voter can terminate the entire process without losing any money before the joint transaction appears on the blockchain, it shows that the whole process is in hand of one voter and if the voter is compromised he can destroy the entire voting process. Moreover, the complexity of the protocol mainly lies in the use of *n-n* threshold signature scheme. To create such a signature securely, one needs to add a verification part for their messages to prove good behaviour, which adds new complexity. Likewise, the ZKP setup requires MPC and "yes/no" voting can limit the adoption of this voting system.

4.2. Agora

In 2015, [2] presented a commercial end-to-end verifiable setup called AGORA, which is composed of four layers: a bulletin board, Catena, bitcoin blockchain, and

Votapp. Agora uses ElGamal cryptosystem for vote casting and cast-or-challenge validation to carry out cast-as-intended validations. Neff shuffling technique along with a ZKP is used to obtain a new list of anonymized ballots. Agora's voting system provides the ability to audit election results at any stage of the voting process and allow anyone to observe an election. A final attestation is signed with the auditors' private key once the election is verified. However, it relies on third parties for supervision, who can conspire with the candidate to alter the votes. Furthermore, the platform is not very precise, offering different alternatives for each stage and does not offer coercion resistance, nor it is a robust voting system.

4.3. A smart contract for boardroom voting with maximum voter privacy [3]

McCorry et al. (2017) proposed the first implementation of a decentralized and self-tallying protocol using Ethereum blockchain, and introduced an additional round of commitment to obtain the fairness property. The protocol does not depend on any central party for the privacy of voters, it can only be exposed through a full collusion attack. However, the unsupervised protocol does not provide coercion resistance therefore, it is only suitable for low coercion elections. Furthermore, the efficiency of system is low since it can scale to a maximum of 40 voters due to the gas limit per block and the identities of voters are publically known. Two major scaling issues are: direct storage of all eligible voters on the smart contract, and the utilization of ECC through an external library made it expensive and too large to store on the blockchain.

4.4. Decentralized Voting: A Self-tallying Voting System Using a Smart Contract on the Ethereum Blockchain [4]

Yang et al. (2018) presented a decentralized, ranked-choice, and self-tallying system using a smart contract on Ethereum blockchain. The proposed system ensures voter confidentiality by using ElGamel homomorphic encryption. The content of the vote is encrypted but signature and identification are in plaintext so anyone can verify the identity and helps to avoid double voting. However, it does not offer receipt freeness and ElGamal encryption requires two exponentiations. It also assumes that every registered voter submits their valid vote, if this would not be the case, any voter can destroy the tallying phase without submitting his vote. And, the current protocol does not solve the scaling issue.

4.5. SHARVOT: secret SHARe-based VOTing on the blockchain [5]

Bartolucci et al. (2018) proposed a blockchain based e-voting system called SHARVOT that uses Shamir's secret sharing scheme and bitcoin blockchain, enables on-chain submission of votes and determination of the winning candidate. To improve privacy, the protocol relies on CircleShuffle technology to unlink the voters from their submitted ballots. The protocol has introduced the voting fee to avoid the Sybil attack. However, all stages of the proposed protocol depend on a single dealer; if this dealer is compromised, the entire voting system can be destroyed. Furthermore, the protocol uses a P2SH address during the vote commitment transaction, which leads to a natural limitation on the size of the script allowed to generate P2SH output address. A reduction of the script size might be done with MAST.

4.6. Platform-independent secure blockchain-based voting system [6]

Yu et al. (2018) proposed a platform-independent verifiable and secure voting system deployed on the BFT-blockchain platform using Hyperledger Fabric. The authors have used Paillier encryption, proof of knowledge, and short linkable ring signatures to ensure security, privacy, and scalability. The trustworthiness of blockchain is achieved by using the 4 validation nodes. However, the generation and uploading of encryption of zeros required for receipt freeness consumed most time. Voter registration is done by the smart contract using an email/ ID/ URL along with the desired password which is a very weak method. Therefore, the protocol is not coercion resistant since any coercer can vote instead of the voter by simply hacking their secret key. It is also claimed that the protocol does not depend on the central party, yet the administrator is responsible for generating the keys used to encrypt and decrypt the ballot. This means that the protocol must trust the central party. If the administrator collaborates with one of the candidates, he can make changes to the results before the results are published.

4.7. Follow My Vote (FMV) [7]

FMV proposed a commercial voting platform that uses the BitShares blockchain as a ballot box and ECC to maintain anonymity. A trusted authority verifies the identity of each voter, authorizes only eligible voters to cast their ballots, and provides them with pass-phrases needed in case of changing their vote. It utilizes two key pairs per voter; for identity verification, and to cast a vote that allows individual verification. However, FMV allows the voter to print a receipt of their transaction and ultimately to audit the casted ballots. It does not offer any mechanism that allows observers to verify the accuracy of the final result. Moreover, a trusted party is needed to ensure voter privacy and hide the link between the voter's identity and voting key, and this party has the ability to change votes since it has all voter's pass-phrases. Finally, votes are cast without being encrypted.

4.8. Verify-your-vote: A verifiable blockchain based online voting protocol [8]

Chaieb et al. (2018) proposed an e-voting system called Verify-Your-Vote (VYV) on the Ethereum blockchain using

elliptic curve cryptography, pairings, and identity-based encryption, but the protocol design does not support coercion- resistance. The security of VYV is proven through the use of verification tool "Proverif". The structure of the ballot allows the voter to save the counter value of the corresponding candidate and use it for verification. Though, the system does not resist coercer attack, and the choice of tallying authorities responsible for decryption of votes and counting is not defined. Also, side-channel attacks can undermine the security that ECC is supposed to provide.

In 2020, [18] designed and implemented a verifiable blockchain-based e-voting system (VYV) and evaluates its security properties and performance. The result shows that the time is linear with the number of voters when there is a single server, and it decreases when the number of servers increases. The same pattern holds for the counting phase, so the worst case is when one tallying authority has to count all votes.

4.9. Ring signature based voting on blockchain [9]

Kugusheva and Yanovich (2019) proposed a private blockchain-based voting system that uses LRS to transfer the secret data without compromising voting reliability and voter privacy. The scheme achieves trust and stabilization using the Exonum framework, which is systematically decentralized. However, it is neither user-friendly nor cost-effective. Moreover, it does not achieve receipt freeness and coercion resistance.

4.10. DABSTERS: Distributed Authorities using blind signature To Effect Roust Security in e-Voting [10]

Chaieb et al. (2019) solved some of the weaknesses of VYV namely the centralized registration method and the problem related to Ethereum where any dishonest miner can modify the transaction before it is stored on the blockchain. The proposed decentralized e-Voting system is based on a private blockchain called DABSTERS and uses a blinded signature algorithm to preserve the privacy of the voter. However, the voter has to go to the office physically to register for authentication. Moreover, no coercion resistance is achieved due to the counter values created by the election authorities, and the scalability and performance of protocol are not checked.

4.11. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability [11]

Zhang et al. (2019) proposed a blockchain-enabled e-voting system called Chaintegrity that satisfies nine properties ranging from scalability, verifiability, robustness, and cost-effectiveness. The authors also proposed a hybrid data structure that combines Bloom filter and Merkle hash tree for fast authentication. Blind signature and Pailler homomorphic encryption are used for large-scale elections to ensure privacy and authenticity. However, the system is proposed for low coercion resistance and three rounds of interaction between the voter and the protocol are required. The selection of election holders to register a voter depends on cryptographic sorting, but it is difficult to generate a random number in a distributed blockchain. Therefore, this feature is not very useful practically. The protocol does not achieve receipt freeness and untraceability, since the voter can use the blind factor in his ballot to prove later how he voted. Finally, the voter has to create two accounts during the registration and casting phase, and also smart contract consumes time in search for a particular transaction, results in a low authentication process.

4.12. Provotum: A blockchain based and end-to-end verifiable Remote Electronic Voting System [12]

Killer et al. (2020) proposed a practical design for a fully decentralized remote electronic voting called Provotum and used public permissioned blockchain as a public bulletin board where only authorized parties can sign the block but anyone can verify it. Therefore, the trust is distributed across different nodes of the blockchain. Provotum is powered by the smart contract, distributed key generation, homomorphic encryption, and cooperative decryption. However, the protocol does not provide coercive security or receipt freeness and support only single voting type. The protocol considers many participants and primitives which leads to an increase in cost and time. Long term privacy cannot be guaranteed as it is based on the security of ElGamal cryptosystem, that is breakable by using the quantum computers in the future. Scalability is not achieved due to the choice of the underlying blockchain and insecure communication channel.

4.13. Scalable Open Vote Network on Ethereum [13]

Seifelnasr et al. (2020) presented an extended version of the work by McCorry et al. and solved scalability problem and universal verifiability by through verifiable off-chain computations using the Merkle tree. The protocol relies on an untrusted administrator to tally the vote off-chain and to publish a Merkle tree of encrypted votes. Its correctness can be publically verified during the dispute phase even if there is only one honest voter, but the amount of gas required in the dispute phase increases linearly with the number of voters, since two Merkle proofs must be performed in addition to two elliptic curve operations. On the other hand, the transaction cost of voter registration includes a Merkle proof of membership, which increases the gas cost. Finally, the total gas needed to run the elections is very low compared to McCorry, but according to the current price, it is still too expensive to be used in large-scale elections.

4.14. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting [14]

Dimitriou (2020) proposed an electronic voting system based on the Bitcoin blockchain infrastructure. The use

of a token randomizer that acts as a black box during the creation of a ballot ensures receipt-freeness and coercion resistance but, it violates the actual definition of coercion resistance since it does not consider the case when coercer is physically present. Universal verifiability is achieved through the append-only structure of the blockchain. Finally, the proposed system combines the features of blockchain with cryptographic primitives: zk-SNARKs and Pederson commitment to establish the sure elections. It is claimed that the voting system places minimal trust in the election authorities. However, it is assumed that the election authorities who handed the token randomizer to the user are not malicious which involves trust in the election authority. Secondly, the construction of zk-SNARKs again requires a trusted party to generate the CRS. If the election authority responsible for creating CRS is malicious, it can create a CRS that breaks the property of ZK and thus learns the information about the voter's secret parameters. Furthermore, tallying time has linear complexity, and finding shows that proof generation takes under 3 min.

4.15. AMVChain: authority management mechanism on blockchain-based voting systems [15]

Li et al. (2021) presented an e-voting system based on an authority management mechanism. This is a 3-layer access control architecture, where a smart contract is used at each layer for validation and granting permissions. The developed system is based on the hyperledger fabric (consortium blockchain). LRS is used to ensure privacy and encrypt the ballot to disconnect the ballots and voters. The proposed system is suitable for enclosed environment like universities since most of the part relay on the smart contract. There is no method specified for the identity check and registration, and any eligible voter can cast a vote instead of candidate as they have an access to candidate's private key. By using LRS, signing time increases according to the size of ring and tallying time increases with the number of candidates, which increases the risk of result tempering.

4.16. Æternum: A Decentralized Voting System with Unconditional Privacy [16]

Killer et al. (2021) proposed a remote electronic voting system that provides unconditional privacy. Æternum does not need to rely a central party instead unconditional privacy is achieved by using the public permissioned distributed ledger. However, it only allows single voting type and does not prevent a replay attack. Fairness is not achieved by default as the ballots are not encrypted. The method is secure with respect to current and future quantum attacks but if the voting client is compromised, the attacker can link any ballot generated with the client to the owner's device.

4.17. A Manipulation Prevention Model for Blockchain-Based E-Voting System [17]

Tas et al. (2021) proposed a double-layer encryption model to avoid the manipulation of voting results, and utilized a decentralized version that ensures privacy and stores the recorded votes in a distributed manner. However, due to the encryption and distribution, the time to distribute the data increases with the number of nodes. Also, the risk of tampering increases if the lower value is chosen for the threshold. Replay attack, Sybil attack, man-in-the-middle attack, and buying attack is possible. Finally, based on the token used in the transaction, an attacker can coerce the voter to vote for a particular candidate and can verify his vote later.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	Platform	Cryptographic primitive	Decentralization	Voting type	Authentication	Tallying protocol
[1]	✓	–	×	–	✓	✓	×	✓	–	–	✓	✓	✓	Bitcoin	ZKP, Threshold signature scheme	No admin	Single	Plain	Blockchain
[2]	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	×	×	✓	Bitcoin	ElGamal cryptosystem	Multi admin	–	–	Any third party
[3]	✓	✓	×	×	✓	✓	×	✓	–	–	×	–	×	Ethereum	Schnorr ZKP, 1-out-of-2 ZKP	No admin	Single	Smart contract administrator	Self-tallying
[4]	✓	×	×	✓	✓	✓	×	✓	×	–	–	✓	×	Ethereum	ElGamal HE, ZKP, distributed encryption	Election admin	Multiple	–	Self-tallying
[5]	✓	✓	×	✓	✓	×	×	✓	–	✓	×	✓	✓	Bitcoin	Secret Sharing, CircleShuffle	Single admin	Multiple	Single dealer	–
[6]	Claimed	✓	×	–	✓	✓	✓	×	✓	✓	Claimed	×	✓	Hyperledger Fabric	PoK, SLRS, Pailler encryption	Single admin	Multiple	SLRS	Administrator
[7]	✓	✓	×	✓	✓	×	✓	×	×	–	×	–	✓	BitShares	ECC	Registrar	Multiple	Trusted dealer	Authority
[8]	✓	✓	–	✓	✓	✓	×	✓	✓	✓	×	✓	✓	Ethereum	ECC, pairings, identity-based encryption, Pailler encryption	Single admin	Multiple	Administrator	Authorities
[9]	✓	✓	✓	×	–	–	×	–	×	–	×	✓	✓	Exonum	LRS	Organizer	Multiple	KYC	–
[10]	✓	✓	✓	✓	✓	✓	×	✓	–	×	×	✓	✓	PBFT blockchain	IBE, Blind signatures	Authorities	Multiple	Digital signature	Authority
[11]	✓	✓	✓	✓	✓	✓	linear	✓	×	×	low	–	×	Platform independent	Blind signature, homomorphic encryption,	Partially	Multiple	Hybrid data structure	Smart contract, election holders
[12]	✓	–	–	✓	✓	✓	×	✓	–	×	×	✓	✓	Public permissioned	ZKP, ElGamal HE, DKG	Authorities	Single	Identity provider	Authorities
[13]	✓	✓	–	✓	✓	×	Claimed	✓	–	–	–	✓	×	Private Ethereum	Schnorr ZKP, OVN, ECC	Untrusted admin	Multiple	Not mentioned	Untrusted admin
[14]	✓	✓	×	✓	✓	✓	×	✓	✓	✓	Claimed	✓	×	Bitcoin	Zk-SNARKs, Pederson Commitment	Registrar	Multiple	Self-authentication	any interested party
[15]	✓	✓	✓	✓	✓	×	×	✓	–	✓	×	✓	✓	Consortium blockchain	LRS	No admin	Multiple	Smart contract	Smart contract
[16]	Claimed	✓	×	✓	–	✓	–	×	–	✓	✓	×	✓	Private permissioned	NIZKP	Voting authority	Single	Voting authority	Anyone
[17]	✓	✓	×	✓	✓	✓	×	✓	×	–	–	✓	✓	Private Ethereum	HE, Secret sharing scheme	Authority	Multiple	Registrar	Network nodes

Table ii: comparison between blockchain based e-Voting schemes

5. Conclusion

e-Voting systems started in 2000, and public blockchains get popularity from 2009-2016. Since 2017, private blockchains have been used more in practice as they are more reliable. Consortium blockchain frameworks like Hyperledger Fabric and Exonum offer more transparency and audibility. By the end of 2019, almost all solutions now rely on permissioned (private) blockchains. We have seen that cryptographic primitives have their limitations concerning privacy and not all blockchain based protocols have succeeded to deliver that level of satisfaction to the voter, which they promised or at least claimed, so the current technologies are not problem-free, there are many unsolved directions like risk of large-scale fraud, strong attack on privacy, and scalability issues, decentralization, quantum attacks that are yet to be addressed. There are some second layer technologies that have been proposed recently such as Sharding, rollups, etc. that could help in one direction and advanced cryptographic primitives on the other.

Reference:

[1] Zhao, Z., & Chan, T. H. H. (2015, December). How to vote privately using bitcoin. In *International Conference on Information and Communications Security* (pp. 82-96). Springer, Cham.

[2] *Agora: Bringing voting systems into the digital age*. Agora. (n.d.). https://www.agora.vote/. Accessed 11 June 2021.

[3] McCorry, P., Shahandashti, S. F., & Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security* (pp. 357-375). Springer, Cham.

[4] Yang, X., Yi, X., Nepal, S., & Han, F. (2018, November). Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain. In *International Conference on Web Information Systems Engineering* (pp. 18-35). Springer, Cham.

[5] Bartolucci, S., Bernat, P., & Joseph, D. (2018, May). SHARVOT: secret SHARe-based VOTing on the blockchain. In *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain* (pp. 30-34).

[6] Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M. H. (2018, September). Platform-independent secure blockchain-based voting system. In *International Conference on Information Security* (pp. 369-386). Springer, Cham.

[7] Long, _ W., & Hourt, _ N. (2021, May 11). *Secure Decentralized Application Development*. Follow My Vote. https://followmyvote.com/.

[8] Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2018, October). Verify-your-vote: A verifiable blockchain-based online voting protocol. In *European, Mediterranean, and Middle Eastern Conference on Information Systems* (pp. 16-30). Springer, Cham.

[9] Kugusheva, A., & Yanovich, Y. (2019, December). Ring Signature-Based Voting on Blockchain. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications* (pp. 70-75).

[10] Chaieb, M., Koscina, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019, July). DABSTERS: Distributed Authorities using Blind Signature To Effect Robust Security in e-voting. In *International Conference on Security and Cryptography (SECRYPT)*.

[11] Zhang, S., Wang, L., & Xiong, H. (2020). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, *19*(3), 323-341.

[12] Killer, C., Rodrigues, B., Scheid, E. J., Franco, M., Eck, M., Zaugg, N., ... & Stiller, B. (2020, November). Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System. In *2020 IEEE 45th Conference on Local Computer Networks (LCN)* (pp. 172-183). IEEE.

[13] Seifelnasr, M., Galal, H. S., & Youssef, A. M. (2020, February). Scalable open-vote network on ethereum. In *International Conference on Financial Cryptography and Data Security* (pp. 436-450). Springer, Cham.

[14] Dimitriou, T. (2020). Efficient, coercion-free and universally verifiable blockchain-based voting. *Computer Networks*, *174*, 107234.

[15] Li, C., Xiao, J., Dai, X., & Jin, H. (2021). AMVchain: authority management mechanism on blockchain-based voting systems. *Peer-to-peer Networking and Applications*, 1-12.

[16] Killer, C., Knecht, M., Müller, C., Rodrigues, B., Scheid, E., Franco, M., & Stiller, B. Æternum: A Decentralized Voting System with Unconditional Privacy.

[17] Taş, R., & Tanrıöver, Ö. Ö. (2021). A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Security and Communication Networks*, *2021*.

[18 Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2021). Design and practical implementation of verify□your□vote protocol. *Concurrency and Computation: Practice and Experience*, *33*(1), e5813.

[19] Delaune, S., Kremer, S., & Ryan, M. D. (2005, September). Receipt-freeness: Formal definition and fault attacks. In *Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy*.

[20] Haines, T., & Smyth, B. SoK: Surveying definitions of coercion resistance.

[21] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

[22] Esteve, J. B., Goldsmith, B., & Turner, J. (2012). International experience with e-voting. *Norwegian E-Vote Project. International Foundation for Electoral Systems. Document disponibil online la adresa http://www. ifes. org/Content/Publications/News-in-Brief/2012/June/% 7E/media/B7FB434187E943C18F4D4992A4EF75DA. pdf*.

[23] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE.

[24] Radwin, M. J., & Klein, P. (1995, December). An untraceable, universally verifiable voting scheme. In *Seminar in Cryptology* (pp. 829-834).

[25] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, *18*(1), 186-208.

[26] Liu, J. K., & Wong, D. S. (2005, May). Linkable ring signatures: Security models and new schemes. In *International Conference on Computational Science and Its Applications* (pp. 614-623). Springer, Berlin, Heidelberg.

[27] Rivest, R. L., Shamir, A., & Tauman, Y. (2001, December). How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 552-565). Springer, Berlin, Heidelberg.

[28] Tieng, D. G., & Nocon, E. (2016, March). Some Attacks on Shamir's Secret Sharing Scheme by Inside Adversaries. In *Conference Proceedings-The DLSU Research Congress* (pp. 7-9).

[29] Langer, L., Jonker, H., & Pieters, W. (2010, December). Anonymity and verifiability in voting: understanding (un) linkability. In *International Conference on Information and Communications Security* (pp. 296-310). Springer, Berlin, Heidelberg.

[30] Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security*, *88*, 101654.

[31] Klarin, A. (2020). The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions. *Research in International Business and Finance*, *51*, 101067.

[32] Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2014). Succinct non-interactive zero knowledge for a von Neumann architecture. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp. 781-796).

[33] Danger, J. L., Guilley, S., Hoogvorst, P., Murdica, C., & Naccache, D. (2013). A synthesis of side-channel attacks on elliptic curve cryptography in smartcards. *Journal of Cryptographic Engineering*, *3*(4), 241-265.

[34] Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

[35] De Keyser, T. (2017). Implementation of a verifiable mix network based on the trade-off between resilience, scalability, and performance.

[36] Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology* (pp. 199-203). Springer, Boston, MA.

[37] Beimel, A. (2011, May). Secret-sharing schemes: A survey. In *International conference on coding and cryptology* (pp. 11-46). Springer, Berlin, Heidelberg.

[38] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

[39] Savu, L. (2012). Signcryption scheme based on schnorr digital signature. *arXiv preprint arXiv:1202.1663*.

[40] Heiberg, S., & Willemson, J. (2014, October). Verifiable internet voting in Estonia. In *2014 6th international conference on electronic voting: Verifying the vote (evote)* (pp. 1-8). IEEE.

[41] Fouard, L., Duclos, M., & Lafourcade, P. (2007). Survey on electronic voting schemes. *supported by the ANR project AVOTÉ*.

[42] Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (pp. 1535-1553).

[43] Noether, S. (2015). Ring SIgnature Confidential Transactions for Monero. *IACR Cryptol. ePrint Arch.*, *2015*, 1098.