



Journal Homepage: [-www.journalijar.com](http://www.journalijar.com)

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/12225
DOI URL: <http://dx.doi.org/10.21474/IJAR01/12225>



RESEARCH ARTICLE

BLOCKCHAIN AS AN E-VOTING TOOL

Jihad Fraij¹, Ashraf Aldabbas² and Nemer Aburumman¹

1. University of Debrecen, Doctoral School of Management and Business, Department of Business Informatics, Debrecen, Hungary.
2. University of Debrecen, Doctoral School of Informatics, Department of Information Technology Systems and Networks.

Manuscript Info

Manuscript History

Received: 25 October 2020

Final Accepted: 28 November 2020

Published: December 2020

Key words: -

Voting System, E-voting, Ethereum,
Blockchain Jordan

Abstract

Blockchain as a distributed system that confirms security and reliability have started a new era of a solid and consensus system. Blockchain's focus on cryptocurrency is encouraging many other processes to follow the same reliable approach of security. Almost all procedures and operations are now invited to be electronically performed in the digital Ethereum network that has been presented. Moreover, this study proposed the use of an Ethereum network on a blockchain platform in the study when it was moved to a blockchain network to confirm transparency. An E-voting system sample has been tested by using an Ethereum network smart contracts in which solidity language and wallets were used. In the voting test, the Ethereum blockchain will be able to collect records in which voters can use their Ethereum wallets or android devices to submit their votes in a consensus node. The researchers studied the voting system taking Jordan as a case study. This study recommended the adaptation of e-voting to support transparency and voters' trust to reduce corruption and unreliability in the voting processes. Moreover, the use of this system will allow a voter to vote from home in the time of the pandemic.

Copy Right, IJAR, 2020, All rights reserved.

Introduction:-

Financial transactions have been revolutionized by the use of Blockchain technology with the beginning of its practical appearance in 2009 (Nakamoto, 2008). The success of using blockchain technology in the financial field led to the expansion of the use of applications that rely on this technology to other areas and fields due to the high transparency provided by this technology.

The use of this technology practically began in 2009 with the emergence of the currency (Bitcoin), which is an electronic currency that is traded between users directly over the network immediately and without the need for any central intermediary authority (government or banks) to complete financial transactions. The process passes through a process of encryption and verification from other users on the network before storing it in the electronic ledger; because of these advantages provided by this technology, its uses expand significantly in various fields such as storing medical information, registering lands, issuing certificates, etc. (Wood, 2014).

Corresponding Author:- Jihad Fraij

Address:- University of Debrecen, Doctoral School of Management and Business, Department of Business Informatics, Debrecen, Hungary.

In 2015, another currency based on blockchain technology appeared, Ethereum (Ether), which is another electronic currency that works in the same way as Bitcoin, in addition to providing the possibility of producing applications that enable users to keep information in an orderly and verified by smart contracts, as will explain later in this paper (Clack, Bakshi, & Braine, 2016). The information stored by blockchain technology cannot be tampered with or modified illegally, which raises the level of transparency and security for users of this technology, and this feature has made this technology suitable for to be used in areas requiring a high level of transparency and security such as electronic voting. Many researchers have discussed the possibility of using technology to conduct the electronic voting process, and the most significant concern during this process has always been security and transparency. However, the number of studies dealing with reliable techniques and applications such as applications that rely on blockchain technology is still minimal. Several studies highlight successful examples of conducting electronic voting. However, in small or unofficial voting, such as conducting opinion polls or questionnaires on the Internet, the use of these technologies is still very limited and risky for governments and large companies to conduct the electronic voting process primarily and officially.

As we mentioned earlier, using these technologies is still limited to conducting polls, polling, and even taking people's opinions about laws. On the other hand, most governments worldwide still use traditional voting methods using papers and ballot boxes. However, with the progress of technology and the growth in population numbers, traditional voting continues to raise questions about the reliability of people in charge of the conventional voting system, the transparency of the process, the guarantee that the results have not tampered, and finally the cost of holding these elections frequently.

Jordan:

Almost all traditional governmental services, in many countries, are being transformed to become electronically (Rumman & Szilágyi, 2018). Some governments have invested in adapting technologies to implement e-voting in their voting systems. Many studies conducted research on the e-voting systems in developed countries. As a developing country, Jordan still uses the 'paper-based' voting system, and it has been used for decades. However, the traditional parliamentary voting system encounters many problems. Every 4 years, the Jordanian parliament and municipal elections and many committees, governmental boards, and professional unions are being elected. The influence of political money and politicians' influence on the communities and people are challenging issues in Jordan's case. Moreover, the lack of trust in the Jordanian government decisions and the unreliability of the parliament elections' performance. Accordingly, there should be several significant researches to study those challenges in which, an electronic voting system is performed to manage and control the entire election processes. A research paper tested the process of electronic voting at a university in Jordan, considering Jordanian universities as mirrors of the actual community. (Abu-Shanab, Knight, & Refai, 2010) have conducted this research during the student union elections. He tested the e-voting system on 302 Jordanian. The results were tested based on the TAM model and stated that students accepted the e-voting system and trusted the processes. It reduces miscalculation and improves the aptness and honesty of the election processes. (Aljarrah, Elrehail, & Aababneh, 2016) proposed an actual e-voting system depending on the TAM model and studied the Jordanian voters' readiness. In this study, a proposed solution and framework are offered to improve and solve the traditional voting system challenges and problems. In pandemics and social distancing, governments should be smart to quickly adapt these processes and techniques to save time, costs, building voters' trust, and stop political money. These solutions will extract a reliable and correct result, which will reduce corruption and politicians' bad influence on voters. The researchers have clearly searched and studied the laws and by-laws of Jordan. It was clear that this process is not mentioned in any article of the regulations. The Jordanian Independent Elections Committee has also stated that e-voting is not official in the present regulations. To sum up, this research recommended the change of the law and by-laws to allow the use of this trend, especially when technology has become the only safe interaction in the world of pandemics.

Related Work:

Concerning our most crucial inspiration in this mission is to grant an impenetrable and dependable e-voting scheme conceivable using blockchain. Since the user has a pc or a mobile device, or any device that can be connected to the internet, he can be capable of voting in a way which lawmakers and directors or managers will be capable of accessing the people's lowest conclusions. By this, real majority rule government will be accomplished automatically (Çabuk, Şenocak, Demir, & Çavdar, 2017). It is integral to be controlled without problems precisely in little towns, and certainly in more significant cities discovered in degenerate nations. As a enumerate number of truths, it will be less in price, assuming a significant quantity of areas will be covered in this election when considering so many cities (European Commission, 2014).

Moreover, the voters who could be on vacation outside their country can easily share in e-voting. The thought of e-voting is if truth be told, more professional than blockchain. So, all regarded cases so the far-off utilized skill of capability models and central computing skill. Estonia is a fantastic case when someone considers that Estonia's government is a fully online e-voting example, in which they achieved a completely online e-voting arrangement (Hao & Ryan, 2016). The concept of e-voting began for debate within the country in 2001. In which authoritatively begun with the aid of the countrywide professionals within the summertime of 2003 (Braun, 2004). Their method is nevertheless in utilize, with numerous advancements and changes in the unique plot. As detailed, it is as of now fantastically reliable. They utilize smart superior ID cards, and non-public card s have been made thru the government peruses (Alketbi, Nasir, & Talib, 2018). Those who will participate in the elections and have a pc with a web connection can without problems vote.

Moreover, Individuals can also submit requests and points on laws at the parliament's web page (<http://rahvaalgatus.ee>). Requests cautiously marked by using a wise Identity card by way of anyone's wishes backing the proposition. In case requests finished a certain number of persons, they will be examined in the parliament. This how using know-how technology can strengthen people's powers, in which a remarkable and outstanding democracy skills is being achieved. That is another excellent case appearing how using technology can reinforce the popular government. Even though being admitted being fruitful and coming to about 30% penetration rate amid later decisions, the Estonian demonstration has, in some parts, not acceptable. The most essential arrangement, by its nature, has a one-point-of-no success in which attempts of people who are not authorized can get access to data in the system. The adaptability of this machine is another address. As long as Estonia encompasses a commonly small population, it is challenging to gauge in the match that this framework could work smoothly in China for example. Constant use of an ID card and user gadget is not always pleasant, as well refers to the additional fetched of, conveying, and carrying and producing voters. In case, Disseminated Denial of Benefit (DDoS) assaults can damage the servers, laptop program, or databases utilized. In these cases, chairmen of a similar framework can also act badly and take, in case he cannot control, a few vital data amid the election.

Other likely advertisements or format sheets located on the Web the factor to point to that issue such as <https://followmyvote.com/>, Human beings who will vote are mentioning whom they vote to namelessly and to remember any unknown votes by observing the scientific formula. At the same time, they recognize there can be mysterious false votes, and they too comprehend that not each person in the selection announced whom they vote. That is why they put an edge to rate the results. In any case, it does not now appear a proper easy conclusion. Although to be an excellent endeavor, it is proper now a long way from being a to a sturdy arrangement.

One of the few countries that use the e-balloting drift is Switzerland. Switzerland is regarded for its large popular government; everyone who is 18 years old can take a dynamic or inactive phase to decide which one may also be held in numerous different points for many various choices. They have moreover started a legitimate work on a voting framework called inaccessible voting (McCorry, Shahandashti, & Hao, 2017). <http://www.strawpoll.me/is>, an internet surveying illustration that can be used. Instead of an e-voting system may also be a well-regarded and without cost or payment service. It is a straightforward internet site that lets all people initiate questions and replying to others' surveys through votes. It elucidates how capable may e-voting be that all and everybody can effortlessly receive to the elections and employ their votes and announce their preference. Individuals are able to share non-public hyperlinks to anyone already carried out the survey (if they understand the connection), and those who have the connection can vote, and one software program can be used <http://www.strawpoll.me/> trusts folks around that they will no more infringe the election approach decision whereas profiting ease to get right of entry to and utilizing highlights of e-voting.

Subsequently, it cannot be utilized in actual situations, such as deciding on the department's head. To be protected here, in scope of actual voters, replica votes, and non-rejection of votes is relatively feeble at <https://electionrunner.com/>, another illustration of e-voting action is actualized added a versatile application and an internet page which folks make and share the elections with different clients. Individuals can signify who will vote and how lengthy it will be remaining, and after that, they put up this election to be sure of it via those who are checking the election system. However, one nevertheless desires to accept as accurate with the central experts who run the elections Inc. Nevertheless, It is one step absent in having a 100% easy and expert e-voting stage. A desirable complete search for paper offers a strong systematic theoretical blockchain-based on e-voting computers (Takabatake, Kotani, & Okabe, 2016).

The writers additionally considered the counteract for voters can now not be observed, and the voting secrecy through the utilization of a center section among the candidate (wallets) and the voter (wallet) as nicely as the utilize of two-coin sorts for these in-between coins (vote) exchanges. In this case, money (votes) dispatched with the aid of the voters implies are accumulated thru the midway unit and modified to another currency's wallet. At that point, the median unit dispatches the new money to their proper point of disembarkation (candidates). Despite the reality that it could be a fantastically enlightening source, it does not consist of documents regarding placing the layout into action, aside from using Bitcoin and Zero coin as the economic forms or giving a massive speak about.

At the time of composing, few scholarly works are indicating the Ethereum blockchain as a framework of e-voting. In (McCorry et al. 2017), Our essential objective is to center on performance works and assemble our association on a little scale to create our online college elections: office chairs, university minister, or student's committee election. It will be done so that everyone can be tested, maintain the decision dealt with, and college students handle will be entirely online so that everybody may go to vote without problems in university's decisions. Our indispensable commitment to the concept of the online decision in becoming a member of them with the Ethereum blockchain stage.

A conference was made through writers who have proposed a complete and an impervious protocol to utilizing the Ethereum blockchain. Their conference with complex numerical approaches in this way, which needs tremendous computational control, seems it is not always as an interconnection of devices that are embedded in objects, allowing them to send and receive data. We constructed Ethereum showed contacts that permit us to test over the variety of voters at the end of the election. The adopted contract has capacities to give the time and length of the election, just like one hundred twenty minutes or three thousand minutes. Also, to comprise any Ethereum account to be among the elections process confirmation is seen as a distinct sub-problem and it is usually erased from this consideration's scope, as correctly as felony directions. It has been considered that the confirmation is a different -problem and it is erased from the scope of this consideration and legal guidelines.

Implementation and Discussion: -

In this research, the researchers favored the Ethereum environment as a development scheme and the blockchain network. This was due to some considerations related to the following. Bitcoin is only meant to prove the accuracy of coinage transactions or, in other words, the validity. Moreover, the Ethereum network presents a broader domain of used cases, accompanied by the SC ability. Several applications that usually need a web server without it being utilized in utilizing a server. As a result, it is quite challenging to handle or ruin the deliberated software source codes.

Figure1, illustrates the mechanism of the relationship of each party involved in the voting process. Voters should register at the platform being introduced by the organizer. Organizers will check the validation of the voter information from its blockchain database being introduced and give the voter access to sign in. In this step, the smart contract will be established as a voting step and sent to the Ethereum network and blockchain. After being processed, the blockchain block will be established and saved. An independent audit will have access to check the voting process and send feedback to the organizer to make sure that these processes are well processed and introduced. Having this relationship, the organizer will only have access to offer the voter the opportunity to vote and see the results being introduced from the blockchain blocks established. This will give the process a high trust and security from the voter side.

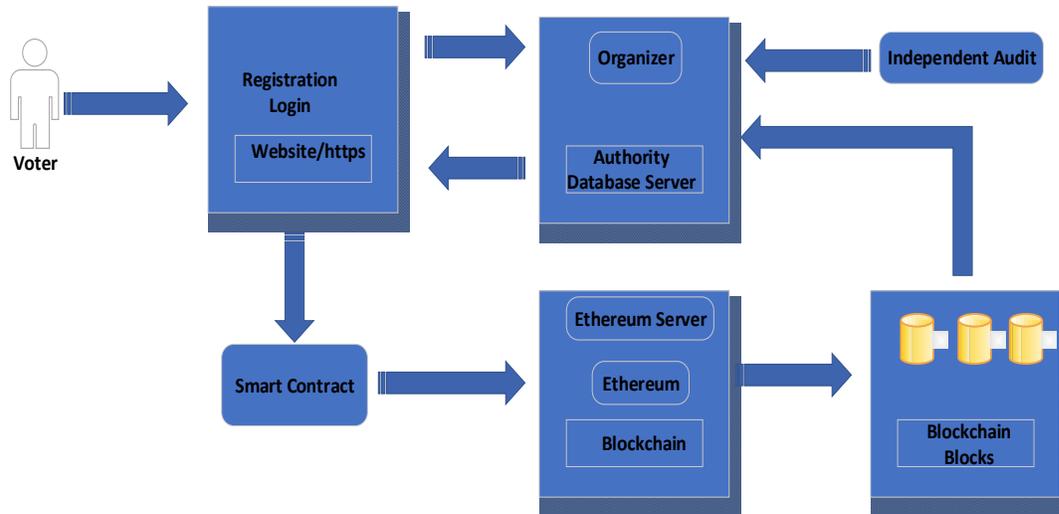


Figure 1:- General overview of the adopted system.

The whole processes which are related to the Ethereum network are expected to become within the actual time. In this case of blocks, the final chain must be written in reciprocity for some Ethers. These are offered as an award to the person who performs these validation processes and writing, exorbitant in the scopes of power and computation time. The authors have determined their (intelligent) Smart Contracts (SC). A durability programming environment should be available to write these contracts. Every 14 seconds, SC is carried out via the Ethereum network peers in which they are also should be validated by a minimum of two other users to be operated. Subsequently, contract functions can be performed and put into effect, and then contracts can be distributed between different members of the group (candidates).

To be able to engage fully online elections, there is a necessity to solve the following troubles. There is an exigency for transparency, the process of authentication, and demonstrability in the voting framework. There is an obligation to guarantee the individuals who are attending the elections. By using this technology, actual people (voters) can use the right credentials that were recognized in the electronic platform. Likewise, governments require the election frameworks are almost 100% translucent as coveted. Thus, there is a need to collect and examine timestamped also signed data of the elections.

These concerns can be cleared up by a peer-to-peer blockchain approach. The researchers can determine the needed SC self-executable among the blockchain quickly. It is just like deploying software. They precisely describe the nature of data models, the scope of rules, objects, and consequently, contracts could be put into effect and executed. In the time following SC are commenced, they could not be outcasted from the blockchain, and individuals can check whether the outcomes of SC implementation are correct or not. Within the Ethereum network, there will be no necessity for a primary power to present the evidence-of-effort. Each of the peers can compute the contracts' outcome with no intervention as the Ethereum network is fit to offer the abstract concept of self-tallying (McCorry et al., 2017).

Within any proportion, utilization of the authentic Ethereum network for inspecting an empirical program associated with such SC's evolution is expensive (as it demands buying some Ethers) and needlessly takes up large system memory. Consequently, the networks of confidential Ethereum are produced and made obtainable to permit the developers to examine their code without crowding the base network.

Among the provided, the code fragment in Figure 2 demonstrates the variable (Voter) description, which is specified as a data type in the robust coding environment. The authors defined the class Voter and gathered Votes in an array. Voters possess several merits and could have additional properties based on the provided use- case schemes. The variable "hasVoted" indicates that if the voter has completed the voting process, the vote will be cast in a lively manner. In a like manner, the variable (vote) accumulates the voter choice from the available candidates, termed

propositions on a wider concept (determined in the role of proposition struct). Moreover, ID is defined as the Ethereum platform wallet address related to the account of the voter within the network of the Ethereum. As an example, any random voter could obtain the below values concerning the associated attributes:

ID: 0xA50965642cdf3C173x8430A3D43EF5CE9673724
HasVoted: true

```

address public presidePerson;
struct Voter {
    bool hasVoted;
    uint256 vote;
    bool eligibleToVote;
    address conformity;
}
struct Proposal {
    uint voteCount;
}

```

Figure 2:- A segment of code to expound the variables and structs.

The variable of address-typed which is related to the "reside person" saves the accountable individual's wallet address, who is the prime person responsible for running the voting process. Anyhow, he/she unable to influence an in progress (or concluded) voting; so, by that he/she owns a privilege to commence the voting action also the voter associated themes that would be allocated to actual voters. By what means this manner executed is provided by Figure 2.

In Figure 3, the grantPrerogativeToVote function can be perceived. The contract proprietor, who was proclaimed once during the contract initialization, is kept in the presidePerson variable. The contract proprietor can uniquely carry out this function. This feature can be inspected via a direct if clause. Afterward, we grant the voting privilege to the entitled voter's (wallet) address. An illustration is provided below:

GrantPrerogativeToVote(0xFA48A37b58E1a3e2F803eC264578bE
B069aA0818);

The individual, who possesses that specific Ethereum address, enjoined via the presidePerson, holds the prerogative to do vote in the current active contract.

```

function grantPrerogativeToVote(address
theVoter) public {
    if (message.sender != presidePerson ||
voters[toVoter].hasVoted){
        return;
    }
    else{
        voters[toVoter].eligibleToVote = true;
    }
}

```

Figure 3:- Code segment to the function that commences voters.

The process of coding the vote () function, is provided by Figure 4, which could be performed by each voter, at which they need to be present at the voting process (unto the finishing time). Voters, when intend to vote, only forward the proposal ID as parameters, then, the registration of votes are confirmed. This process basically reveals the one who is at the same time, trying to perform this contract function. Additionally, in case the person, holds the prerogative to vote and has cast his/her vote. Afterward, the person is flagged in the guise of (has Voted), also the candidate (proposal) vote enumerate is augmented by (1) one or other value depending on the voter weight.

```
function vote(uint8 towardProposal) public {
  Voter storage sender = voters[msg.sender];
  if (sender.isVoted || towardProposal >=
  proposals.length && !sender.eligibleToVote)
  return;
  sender.hasVoted = true;
  sender.vote = towardProposal;
  proposals[towardProposal].voteEnumerate
  += 1;
}
```

Figure 4:- Code segment describing the vote casting operation.

The function of triumphProposal(), which is given in Figure 5, gives back the identity of the triumphing contestant within the variable of (triumphProposal). This will not end the voting operation itself. However, it gives back the triumphing proposal each time it is put into effect. This function examines each proposal, depends on the votes, and after that sends back the person who is the winner among the voting operation within the implementation time, as it will not stop the election.

```
function triumphantProposal() public constant returns
(uint256 _triumphantProposal) {
  uint256 triumphantVoteEnumerate = 2;
  _winningProposal=0;
  for (uint8 pillar = 0; pillar < proposals.length;
  pillar++)
  if (proposals[pillar].voteEnumerate >
  triumphantVoteEnumerate)
  {
    triumphantVoteEnumerate =
    proposals[pillar].voteEnumerate;
    _triumphantProposal = pillar;
  }
}
```

Figure 5:- Code segment that shows the voting process results.

Table 1 demonstrates the test ballots. Here, the time consumed for all voters is computerized. Voter 1 is the only voter who has the privilege to vote first because he generates the test-election. Consequently, other voters should be authorized to vote.

Table 1:- Creation of Contract and Voting Spent Times.

	Contract Origination	Voter-1 Procedure	Voter-2 Procedure	Voter-3 Procedure	Voter-4 Procedure
Voting #One	37s	32s	46s	48s	49s
Voting #Two	31s	31s	44s	43s	43s
Voting #Three	41s	38s	55s	54s	54s
Voting #Four	45s	36s	53s	52s	52s
Voting #Five	1m	31s	27s	27s	27s

It generally appends the time of block creation to the original voting process time. In the table above, the fastest voter in casting votes is voter 1. All contracts can run synchronously, so the third voter does not have to commit to others. The time difference in process monitoring is the creation of the block and the load of work in the network. However, it never overrides for one minute. One of primary issues with blockchain-based electronic voting platform is providing voter anonymity with no impact on the voting process transparency. Basically, transactions (votes, transfers, etc.) are being inserted to blockchain blocks in plain text. For that reason, voting from wallet address X to Y could be perceived by persons who has access to the chain. In fact, a major violation. Moreover, it is unimaginable to use a method like this for critical substantial or elections. Figure 6 shows the creation entry of the voting process.

Figure 6:- Voting process entry creation.

Ensuring this invisibility of users is another main confrontation in the legacy business. Figure 5 demonstrates the entries related to the vote process creation among the blockchain, which is publicly obtainable to any person involved in this scope. Within this work, a solution has been introduced based on the Diffie-Hellman process, in which it refers to using random numbers beside private or public key pairs, hence a "two-round" referendum could be conducted with the privacy of the ballot (Hao & Ryan, 2016). However, this research does not contemplate the blockchain technique; it is not straightforward to endorse for several scenarios; nevertheless, authors of (Hao & Ryan, 2016) have implemented it in order to enforce Ethereum smart-contracts in post examination.

Conclusion:-

In this paper, the researchers made it successful to build a proposed blockchain e-voting platform. It was clear that using the blockchain and Ethereum network will be one of the best options to build trust in the voting system. The proposed system solved the security debates in which Integrity, privacy, and transparency were confirmed. As a distributed system, authorities cannot or will not interfere in the voting records, in which corruption and cheatings

are omitted. The accessibility of voter is vast in which all devices with an internet connection can access and accomplish the voting task in a reliable and secure as well as effective way. If authorities and governments are searching for a voting system in which no internal or external political and/ or governmental interference are available, then the blockchain-based Ethereum network is the perfect solution.

References:-

1. Abu-Shanab, E., Knight, M., & Refai, H. (2010). E-voting systems: a tool for e-democracy. *Management Research and Practice*, 2(3), 264–275.
2. Aljarrah, E., Elrehail, H., & Aababneh, B. (2016). E-voting in Jordan: Assessing readiness and developing a system. *Computers in Human Behavior*, 63, 860–867. <https://doi.org/10.1016/j.chb.2016.05.076>
3. Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services-Use cases, security benefits and challenges. 2018 15th Learning and Technology Conference, L and T 2018, 112–119. <https://doi.org/10.1109/LT.2018.8368494>
4. Braun, N. (2004). E-Voting: Switzerland's projects and their legal framework–In a European context. *Electronic Voting in Europe-Technology, Law, Politics and Society*, Workshop of the ESF TED Programme Together with GI and OCG. Gesellschaft für Informatik eV.
5. Çabuk, U. C., Şenocak, T., Demir, E., & Çavdar, A. (2017). A Proposal on initial remote user enrollment for IVR-based voice authentication systems. *Int. J. of Advanced Research in Computer and Communication Engineering*, 6, 118–123.
6. Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: foundations, design landscape and research directions. *ArXiv Preprint ArXiv:1608.00771*.
7. European Commission. (2014). Final Report: Study on eGovernment and the Reduction of Administrative Burden (SMART 2012/0061) . Retrieved from <https://ec.europa.eu/digital-single-market/en/news/final-report-study-egovernment-and-reduction-administrative-burden-smart-20120061>
8. Hao, F., & Ryan, P. Y. A. (2016). *Real-World Electronic Voting: Design, Analysis and Deployment*. CRC Press.
9. McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. *International Conference on Financial Cryptography and Data Security*, 357–375. Springer.
10. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute. In 2008-10-31. Retrieved from www.cryptovest.co.uk
11. Rumman, N. A., & Szilágyi, R. (2018). Overview of the electronic public services in agriculture in Jordan. *Journal of Agricultural Informatics*, 9(2), 40–53. <https://doi.org/10.17700/jai.2018.9.2.433>
12. Takabatake, Y., Kotani, D., & Okabe, Y. (2016). An anonymous distributed electronic voting system using Zerocoin. *IEICE Technical Report= 信学技報*, 116(282), 127–131.
13. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151(2014), 1–32.