[18] https://drive.google.com/open?id=17SLasy_nomXCNBCf2mda_gO-bKPWx4_s

E-Voting System Using Blockchain

Dr. Richa Sharam
Computer Science and Engineering
Dept, Bhagwan Parshuram Institute
Of Technology, Delhi/India
richasharma@bpitindia.com

Dr. Mugdha Sharma
Computer Science and Engineering
Dept, Bhagwan Parshuram Institute
Of Technology, Delhi/India
mugdhasharma@bpitindia.com

Akanksha Dhamija
Computer Science and Engineering
Dept, Bhagwan Parshuram Institute
Of Technology, Delhi/India
akankshadhamija12@gmail.com

***Abstract*: There’s no doubt about the pervasive impact that digitalization has had on the lives of people, globally. However the electoral system still uses paper in its conventional implementation. The paper based centralized system (offline) has its own disadvantages like lack of transparency and a security threat. The general elections are organized by a centralized authority that has complete access of the database collected, which in turn can be tampered for considerable benefits.**

The revolutionary concept of Blockchain tends to digitally solve the problem due to its decentralized nature. It embraces the decentralized system and not any single authority holds the database. The adoption of blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation. This research discusses the recording of voting result using blockchain algorithm from every place of election. The Ethereum platform is a smart contract that makes blockchain more reliable to be used for products of daily services. Smart contracts are meaningful pieces of codes, to be integrated in the blockchain and executed as scheduled in every step of blockchain updates. On the other hand, evoting is a very volatile and crucial issue, therefore handling it with robust and secure concept of smart contracts turns out to be a viable solution to develop smarter, cheaper, secure, transparent and convenient electoral systems. The major benefit of using Ethereum is its consistency, widespread use and provision of smart contract logics. The system uses proof of work because of the hard to find solution to the problem property and once found, it can be easily verified.

Keywords-: Blockchain; e-voting; Ethereum; security.

I. INTRODUCTION

Blockchain is the dawn of new millennium’s technologies that has a wide bandwidth of applications. The blockchain technology owes its success to the widely accepted and very first cryptocurrency, Bitcoin[1].Studies suggest that the blockchain technology can be used not only for the monetary transactions but also in many other areas due to the high transparency of the system. As sited in Bitcoin, the wallets are in a distributed structure. Therefore, the total amount of coins and transactional volume in the world can be traced momentarily and clearly. This nullifies the need of a central authority or complete the P2P-based system.

Because of this not only money transactions but structural values can also be evaluated and stored in this distributed chain, and can be maintained securely with the help of some cryptologic methods. The most important example for this is the Ethereum coin (Ether) revealing that this technology can produce structured systems with certain modifications [2] as described above. Smart Contracts [3] enforce software programs that are written into blockchain and are immutable. These programs cannot be manipulated once written. Hence, they continue to work autonomously, transparently and properly without involvement of any external stimuli [4].The distributed nature of blockchain might address more issues than the digitalization purpose.

E-voting projects are being studied extensively, some still being used and implemented to find a reliable solution. There are many online polls and petitions being actively implemented into the regime of legislation yet we cannot say the same for elections as they define the democratic element of the constitution of nation and also form the basics of the administrative methodologies. Thus, the democratic society demands a more transparent, robust and secure approach to electoral process.

II. MOTIVATION

The solemn purpose of elections is to channel the sovereignty as a representative of the democracy. Each eligible voter, comes to the polling stations with government issued id proofs, mostly Voter ID cards, gets verified by the committee members and chooses a valid and legitimate option.

Many governmental and organizational election are held using sealed paper ballots, poll booths and EVM (Electronic Voting Machine). The notarized accounts are then counted and results are announced publically. The complete process of counting votes in conventional elections can take 3 to 7 working days depending on the speed of sending the sound to a higher level [5]. The reliability of notaries are at disposal of the committees involved. The most frequent problem in elections is the issue of data manipulation, security, and transparency.

The main motive of the project is to build a robust, reliable and secure e-voting system and show that blockchain is a viable solution to this as availability of an e-voting system will make this available for anyone who has a computer, or a mobile phone and people’s opinion will be more public. When the opinion of public will be easily accessible by the politicians and managers, the society will be lead to the true direct democracy [6]. The e-voting system also promises to cut down the long term cost of conducting elections especially if the distribution is to be made at 1000s of locations involving millions of voters [7]. Also, it can resolve the problem of absenteeism while voting if the voter in unavailable in the region during the voting days due to any reason. E-voting system adds mobility to the voting regime.

III. RELATED WORK

Blockchain and Benefits of Blockchain

Blockchain is a decentralized technology that works on the principle of transparent Data distribution. It stores data record that grow continuously and are not controlled by any single authority. It is an immutable and transparent ledger [8]. It consists of a sequential series of several blocks which are related as hash from the previous block is used in making the next block. Therefore, attempt to change the information will be next to impossible as it will affect the trail [9].

The widely known Blockchain technology currently exists in the Bitcoin system which is the public ledger of all transactions. Bitcoin is a decentralized, peer-to- peer digital payments system based on the first public key cryptography proposed by Satoshi Nakamoto in 2008 [4]. Bitcoin uses a consensus protocol called PoW (Proof of Work) based on cryptocurrency to ensure only legitimate transactions are allowed within the system. Where each transaction is calculated its hash value and entered into a database called Blockchain as described in fig.1. To connect between one block with another block, the hash value of the previous block inserted into the next block then calculated its hash value. The hash value must meet certain requirements called difficulty in order to be considered a legitimate block. Searching for hash values that match those requirements is called Proof Of Work. Bitcoin stores all transaction information in a database called blockchain in the internet network. Blockchain consists of several blocks associated with each other and in sequence as shown in fig.1 The blocks are related because the hash values of the previous block are used in the next block creation process. The effort to change the information will be more difficult because it must change the next blocks.

The first block is called the genesis block.

In creating new blocks, miner required in the mining process using hash computing equipment. Miner compete against each other to create a new legitimate block in accordance with the specified difficulty. A new block is generally generated by a miner but there are times when more than one new block is generated by multiple miners that both meet the criteria even though the odds are small, making blockchain a fork. If this case occurs, then the voting process conducted by the miners

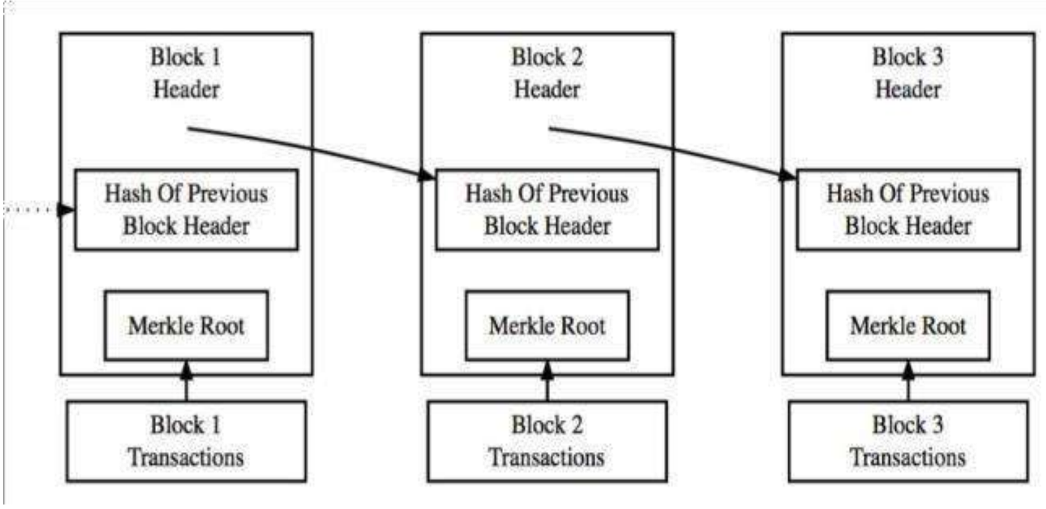


Figure 1. Blockchain Illustration *Source :-www.blockchain.org*

The voting process is done by way of the miner choosing one of several new blocks and then producing the discovery of a longer chain branch. Then the entire Bitcoin system uses the longest branch and deletes all other branches. Unused blocks are called block orphans and become invalid, also all transactions that have been recorded in the block orphan will be inserted into the new block. Blockchain comes with a variety of different types, but has several common elements :

- Blockchain is distributed digitally to a number of computers in almost real time.
- Blockchain is decentralized, the entire recording is available for all users and peer to peer network users. This eliminates the need for central authorities, such as banks, as well as trusted intermediaries.
- Blockchain uses many participants in the network to reach consensus.

Participants use their computers to authenticate and verify every new block. For example, to ensure that transactions not occur more than once, new blocks are only adopted by the network after the majority of its members agree that they are valid.

- Blockchain uses cryptography and digital signatures to prove identity.

Transactions can be traced back to the cryptographic identity, which is theoretically anonymous, but can be re-linked with real-life identity using reverse engineering techniques. • Blockchain has a difficult (but possibly) mechanism for altering stored records.

Although all data can be read and new data can be written, previously existing data on blockcahin can't be changed theoretically unless the rules embedded in the protocol allow such changes by requiring more than 50 percent of the network to approve the change.

- A Blockchain is time-stamped.

Transactions in blockchain are timed, so they are useful for tracking and verifying information

- Blockchain is programmable.

Instructions embedded in blocks, such as "if" this "then" do that "else do this, allow transactions or other actions to be performed only if certain conditions are met, and may be accompanied by additional digital data.

Blockchain has several advantages, which makes it a powerful and secure alternative to distributed databases [8]:

- High Availability: Distributed completely to all nodes and stored in the database completely.
- Verifiability and Integrity: Each block is verified and added to the blockchain. Therefore, it will be difficult to change the data in it because all the blocks have to be changed value. • Easy in determining a common starting point, where to store data - which is always added to the last block in the longest chain.

These advantages make the blockchain attractive for use in recording systems on e-voting.

B.Election and Blockchain Technology

E-voting currently widely used by some countries in the world, for example in Estonia. The country has been using the e-voting system since 2005 and in 2007 conducted online voting and was the first country in the world to conduct online voting [8]. Since then, a legally binding online voting system has been implemented in various other organizations and countries such as the Austrian Federation of Students, Switzerland, the Netherlands, Norway, and so on [9]. But it still has considerable security issues and the selection is often canceled [10]. Although getting a lot of attention, online voting system is still not widely done in various countries around the world. The traditional voting system has several problems encountered when managed by an organization that has full control over the system and database, therefore the organization can tamper with the database, and when the database changes the traces can be easily eliminated [11].

The solution is to make the database public, the database owned by many users, which is useful to compare if there are any discrepancies. The solution to the e-voting system is compatible with using blockchain technology. Blockchain technology allows in support of e-voting applications. Each voter's vote serves as a transaction that can be created into blockchain that can work to track voice counting. In this way, everyone can approve the final calculation because of the open blockchain audit trail, the vote count can be verified that no data is altered or deleted nor is there any unauthorized data entered in the blockchain.

IV. IMPLEMENTATION

Among many choices of different tech stacks in the study it is found that the best suited option for implementing the system is Ethereumblockchain network. It provides the bigger range of use cases with the power of smart contracts, through which many applications which require a web server can be run without it, on a peer to peer network, thus making them very hard if not impossible to mutate.

Another reason of selecting ethereum network is that the transactions happen in almost real time.The transaction on ethereumblockchain occurs in exchange of some ethers or gas which is used to cover the cost of operations, hardware and reward to the miners who verify these transactions. The contracts are written in solidity programming language which is used to develop smart contracts in ethereum.

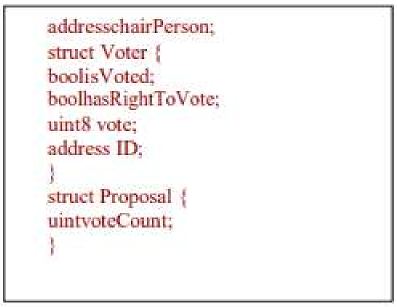
To be able to hold elections following challenges which include transparency,authentication, verifiability and individuality shall be overcome. In order to make transparent and verifiable elections check signed and time stamped data is needed to be gathered and stored. Also,to preserve the individuality it is important to make sure that a person who is eligible to vote in particular election can only vote once and only on his behalf. No person must be able vote on someone else's behalf.

These challenges can be solved by using blockchain by writing executable smart contracts according to the aforementioned challenges. Just like writing a code in any other programming language, one needs to define some rules, exceptions, error handling, objects, data models etc. After a smart contract is initialized it can be removed or discarded for the blockchain, and anyone on the network can verify the execution trail.

To deploy a contract on main ethereum network is costly and requires ether (A crypto currency) which is costly. So for testing purposes the contract has been deployed on a test network. There are many test networks available and one of them is rinkeby (https://www.rinkeby.io/). One can get some fake ethers on this network to deploy and perform transactions on this network. In order to use a test network users need to download a legit ethereumwallet to store and manage their account.

In the code given in the following figure - the Voter has been defined as a struct in the solidity. This structure contains a Boolean variable isVoted to check if the voter has voted before or not hasRightToVote to check if the person has the right to vote or not vote - an integer to select the index of the candidate the person to which the user has voted. ID - to keep the address of the voter.

There is another structure named proposal - which counts the number of votes a candidate or a proposal has got.



```
addresschairPerson;
struct Voter {
boolisVoted;
boolhasRightToVote;
uint8 vote;
address ID;
}
struct Proposal {
uintvoteCount;
}
```

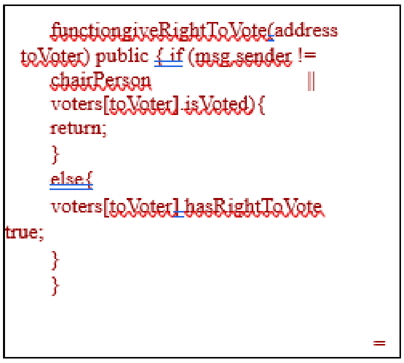
In Fig. 2, giveRightToVote function

Ownerof the contract, who was declared once during theconstruction of the contract is held in the chairpersonvariable. This function can only be executed by the owner ofthe contract. This property can be checked with a basic ifstatement. Then, the voting right to an eligibleVoter’s (wallet) address is given. Example as follows:

giveRightToVote(0xDF69B68b00A3a4e6F907eD

353467bA
C068aF0717);

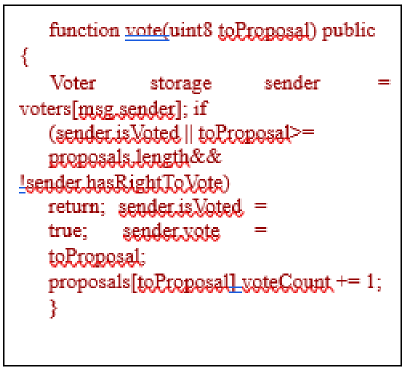
The person, who has that Ethereum address, imposed bythe chairperson, has the right to vote within this contract.



```
    functiongiveRightToVote(address
  toVoter) public { if (msg.sender !=
    chairPerson                    ||
    voters[toVoter].isVoted) {
    return;
    }
    else{
    voters[toVoter].hasRightToVote
true;
    }
    }
                                        =
```

Fig. 3. Code block of the function that initialize voters.

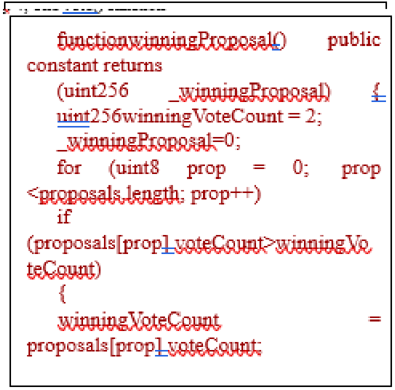
The given code block canbe executed by every voter, whenever they want to attend thevoting (until the deadline). Voters just send the id of theproposal, which they want to vote as a parameter and theirvotes are hence recorded. This function firstly detects who currently are trying to execute that function of the contract.More, if the person has the right to vote, and casted his/hervote, thereafter the person is marked as already isVoted, and the vote count of the candidate (proposal) of his choice isincremented by one or by another number based on his/hervoter weight.



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

F

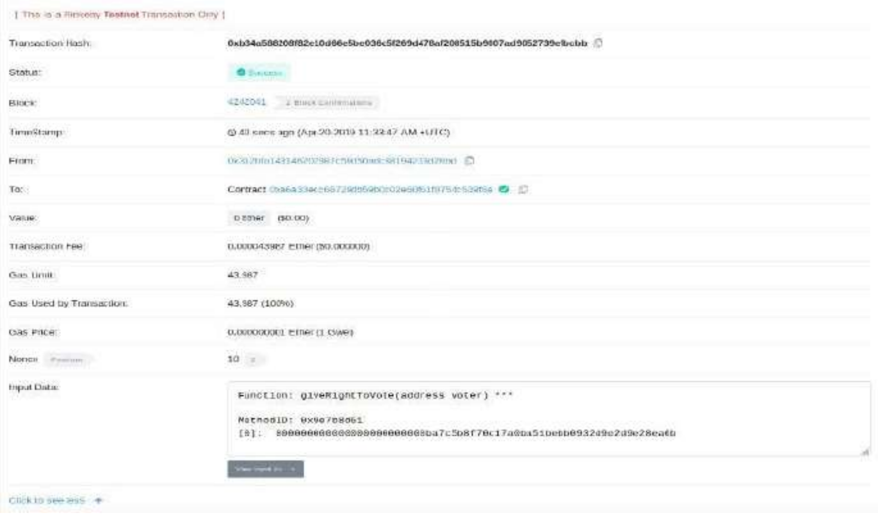
ig. 4, The vote() function



```
    functionwinningProposal()      public
constant returns
    (uint256      _winningProposal)     {
    uint256winningVoteCount = 2;
    _winningProposal=0;
    for    (uint8    prop    =    0;    prop
<proposals.length; prop++)
    if
(proposals[prop].voteCount>winningVo
teCount)
    {
    winningVoteCount                    =
proposals[prop].voteCount;
```

Fig. 5. Code block defining the vote casting process.

The winningProposal() function, presented in Fig. 4, returnsthe id of the winning candidate in the winningProposalvariable. It doesn’t finish the voting process itself, but itreturns the winning proposal every



[This is a Rinkeby Testnet Transaction Only]

Transaction Hash: 0xb34a588208f82e10d86e5be036c5f269d478af208515b9107ad9052739e8cbb

Status: Success

Block: 4242041 [illegible]

TimeStamp: 40 secs ago (Apr-20-2019 11:33:47 AM +UTC)

From: [illegible]

To: Contract [illegible]

Value: 0 Ether ($0.00)

Transaction Fee: 0.000043987 Ether ($0.000000)

Gas Limit: 43,987

Gas Used by Transaction: 43,987 (100%)

Gas Price: 0.000000001 Ether (1 Gwei)

Nonce 10

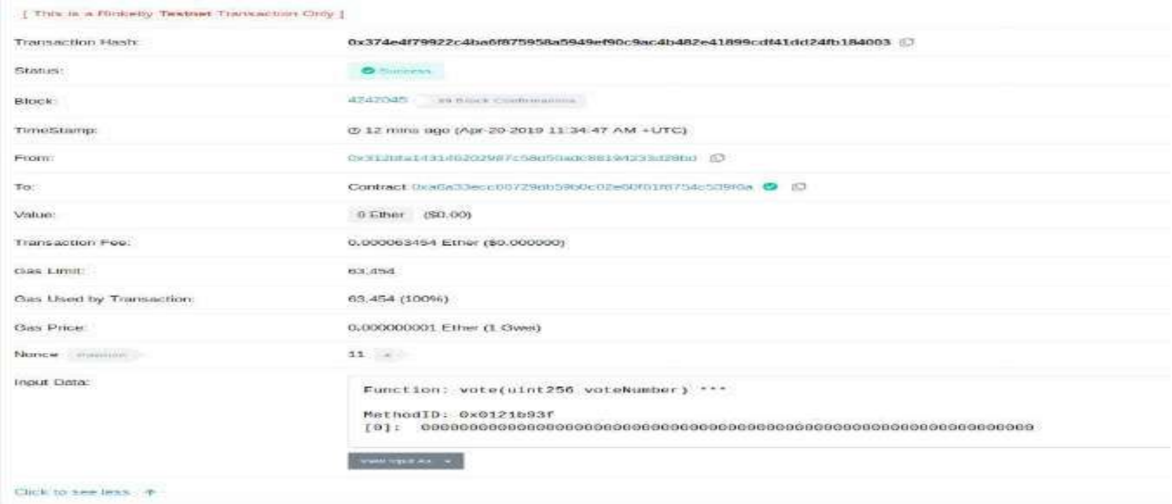
Input Data:

```
Function: giveRightToVote(address voter) ***

MethodID: 0x9e7b8d61
[0]:  000000000000000000000000ba7c5b8f70c17a8ba51bebb0932d9e2d9e28ea6b
```

Click to see less

time it is executed. Thisfunction checks every proposal, counts the votes and thenreturns the one, who is the winner of the whole votingprocess as of the execution time, since it doesn’t end theElection. Voter can verify the trail of the blockchain on the rinkeby network by going to the https://rinkeby.etherscan.io and entering the transaction hash received during the casting of the vote.



[This is a Rinkeby Testnet Transaction Only]

Transaction Hash:	0x374e4f79922c4ba6f875958a5949ef90c9ac4b482e41899cdf41dd24fb184003
Status:	Success
Block:	4242045 [illegible] Block Confirmations
TimeStamp:	12 mins ago (Apr-20-2019 11:34:47 AM +UTC)
From:	0x312bfa1431d02029f7c58d50adc88194233d28bd
To:	Contract 0xa6a33ecc00729db59b0c02e00f01f6754c5d9f0a
Value:	0 Ether ($0.00)
Transaction Fee:	0.000063454 Ether ($0.000000)
Gas Limit:	63,454
Gas Used by Transaction:	63,454 (100%)
Gas Price:	0.000000001 Ether (1 Gwei)
Nonce	11
Input Data:	Function: vote(uint256 voteNumber) *** MethodID: 0x0121b93f [0]: 0000000000000000000000000000000000000000000000000000000000000000

Click to see less

Fig. 6 and Fig. 7 show detailed records of the entries (blocks) regarding the vote creation and casting operations written in theblockchain. This information is publicly available to everyone tracking the network.

V. CONCLUSION

By building this proposed smart contract of ours, success has been achieved in moving e-voting to the blockchain platform and we addressed some of the fundamental issues that legacy e-voting systems have, by using the power of the Ethereum network and the blockchain structure. The trials have resulted in, the concept of blockchain and the security methodology which it uses, namely immutable hash chains, has become adaptable to polls and elections. This achievement may even pave the way for other blockchain applications that have impact on every aspect of human life. At this point, Ethereum and the smart contracts, which made one of the most revolutionary breakthroughs since the blockchain itself, helped to overturn the limited perception of blockchain as a cryptocurrency (coin), and turned it into a broader solution-base for many Internet-related issues of the modern world, and may enable the global use of blockchain.

E-voting is still a controversial topic within both political and scientific circles. Despite the existence of a few very good examples, most of which are still in use; many more attempts were either failed to provide the security and privacy features of a traditional election or have serious usability and scalability issues. On the contrary, blockchain-based e-voting solutions, including the one we have implemented using the smart contracts and the Ethereum network, address (or may address with relevant modifications) almost all of the security concerns, like privacy of voters, integrity, verification and non-repudiation of votes, and transparency of counting. Yet, there are also some properties that cannot be addressed solely using the blockchain, for example authentication of voters (on the personal level, not on the account level) requires additional mechanisms to be integrated, such as use of biometric factors [12].

The prominence of distributed systems stands out especially when considering the mitigation of the risk that storing the registrations at a central location (office). This can always somehow allow officials to have the opportunity to physically access to the vote records, which could lead to corruptions and cheatings by the authorities. Additionally, in today's connected world, with the concept of the Internet of Things (IoT), expectedly, many non-computer devices will gain access to the Internet. While we are still working on a mobile phone application as a supportive extension to our work to widen the usability; it is important to note that, apart from phones and tablets; air conditioning devices, cars, chairs, clothes, refrigerators, televisions, and many other everyday objects are/will be able to directly reach to the internet. In terms of blockchain, it won’t be difficult to build such distributed systems when there is such a large network and a reserve processing power. Moreover, if all these devices work together as a grid to shorten the validation period of transactions in a blockchain, we will be able to do most of our online transactions securely, reliably, and effectively, not only in theory but also in practice.

ACKNOWLEDGMENT

This study is a part of a broader research related to evoting systems, conducted by the research and development group at BhagwanParshuram Institute of Technology, Computer Science and Engineering Department, and has been supported by Dr. DeepaliVirmani, Head of Department, Computer

Science and Engineering and Ms. AkankshaDhamija, Assistant Professor, Computer Science and Engineering Department.

REFERENCES

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: https://bitcoin.org/bitcoin.pdf .

[2] G. Wood, "Ethereum: a secure decentralisedgeneralised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[3] C.D. Clack, V.A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions", Mar 2017, arXiv:1608.00771.

[4] E. Maaten, "Towards remote e-voting: Estonian case", Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.

[5] Christian, "Desain Dan Implementasi Visual Cryptography PadaSistem E-Voting UntukMeningkatkan Anonymity," InstitutTeknologi Bandung, 2017.

[6] U.C. Çabuk, A. Çavdar, and E. Demir, "E-Demokrasi: YeniNesilDo÷rudanDemokrasiveTürkiye'dekiUygulanabilirl i÷i",[Online] Available: https://www.researchgate.net/profile/Umut_Cabuk/ publication/308796230_E- Democracy_The_Next_Generation_

Direct_Democracy_and_Applicability_in_Turkey/links/5818a6d408a ee7cdc685b40b/E-Democracy-The-Next-

Generation-DirectDemocracy-and-Applicability-in- Turkey.pdf.

[7] "Final report: study on eGovernment and the reduction of administrative burden (SMART 2012/0061)", 2014, [Online]. Available: https://ec.europa.eu/digital-single- market/en/news/finalreport-study-egovernment-and- reduction-administrative-burdensmart-20120061.

[8] D. A. Wijaya, *Bitcoin Tingkat Lanjut*. 2016.

[9] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain," *2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015*, pp. 577–578, 2016.

[10] T. Martens, "Verifiable Internet Voting in Estonia," *October*, pp. 1– 7, 2009

[11] Follow My Vote, "Why Online Voting." [Online]. Available: https://followmyvote.com/. [Accessed: 01-Jan-2017].

[12] U.C. Çabuk, T. ùenocak, E. Demir, and A. Çavdar, "A Proposal on initial remote user enrollment for IVR-based voice authentication systems", Int. J. of Advanced Research in Computer and Communication Engineering, vol 6, pp.118- 123, July 2017.