E-VOTING SYSTEM USING BLOCKCHAIN

Raj V Garag[1], Akhil Krishna[2], Dr.Padmashree T[3]

[1]Student, Dept. of ISE, R V College of Engineering, Bangalore
[2]Student, Dept. of ISE, R V College of Engineering, Bangalore
[3]Assistant Professor, Dept. of ISE, R V College of Engineering, Bangalore

---

Abstract - *Voting plays a big part in creating a democratic society. Traditional voting requires electors to vote in designated polling stations, which typically entails huge time and expense budget expenditure. E-voting, a modern comprehensive electronic voting method based on the technique of cryptography, was slowly adopted and promoted by individuals. The program allows full-function online voting by general household computers, and will automatically and anonymously count the entire polling results. Compared to conventional elections, electronic voting is more accountability and impartiality addresses of the economic system.*

As an e-voting program the Internet platform depends mainly on. The key obstacle for e-voting is the serious security risks it might pose. Various procedures related to ballot secrecy, person verifiability, availability, completeness, fairness, uniqueness, robustness, universal verifiability and receipt-freeness have been widely introduced in order to minimize risks over the past 40 years. The implementation of e-voting in digital currency has slowly become mature nowadays.

Based on the participants' specific safety criteria, this paper proposed a blockchain-based protocol aligned with ballot-privacy objectives, verifiability, accessibility, completeness, uniqueness, robustness, and coercion-resistance.

Key Words: E-VOTING, Block Chain, Ring Signature, Electoral Authority(EA), Bit coin Address Pool, Cryptography

1. INTRODUCTION

In 2008, Bitcoin inventor S.Nakamoto published a paper[23] to define a peer-to-peer-based crypto-currency network. The Bitcoin has modified the cash payment system conventional way. Blockchain technology has attracted people's interest with the launch of the Bitcoin. The blockchain is a decentralized ledger, the new ledger can be synchronized into local by all individuals and they have no permission to tamper with the decentralized ledger material.

1.1 PROPERTIES

The blockchain has the properties of decentralization, mutual trust, universal maintenance, data security, privacy protection since the inception of the blockchain. It has been without precedent and its growth is very rapid.

• Decentralization: It decentralizes the blockchain. There are no central computing devices which store the transaction ledger. Each blockchain node stores the same copy.

• Difficult to forge: Every block should be distributed to every node around the world due to its decentralization.

• Traceable Transaction: Every transaction is free and transparent in the blockchain. Each transaction information includes the address of the sender and the address of the receiver which can be traced by anyone.

We also suggested a Bitcoin based protocol in this article. Everybody can access the details from the blockchain for any transaction. Every Bitcoin address in the Bitcoin has no connection to their personal identity. The blockchain is thus pseudonymous to everyone and has the open transactions, which have the same e-voting property specifications.

1.2 MECHANISM

A collection of peer-to-peer nodes makes up the blockchain. It conserves the precision of the data for each node by running a consensus algorithm. The Bitcoin is a standard representation of the blockchain, to define the blockchain function. We should have a clear description of blocks, to describe the blockchain. The block consists of the block header and the block's main portion including a raw serialized transaction. The raw transaction includes the unique identifier(TxID) which is the transaction's hash value. Growing Merkel tree leaf node constitutes the identification value of all transactions on each block.

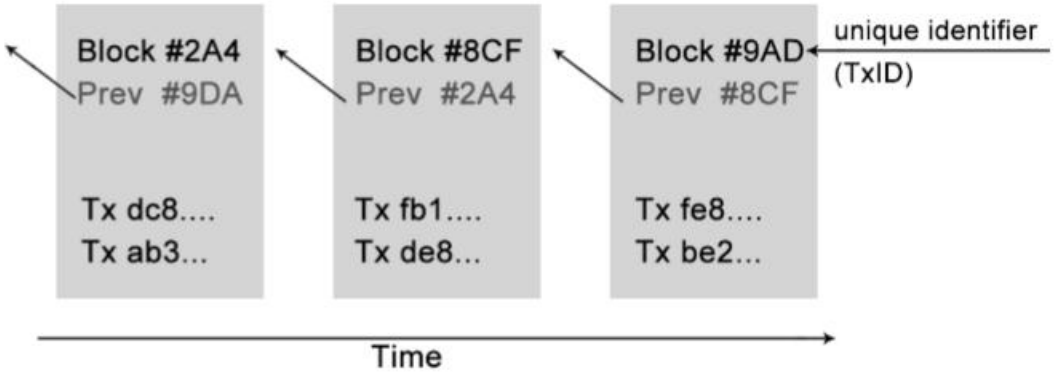

Figure 1.1: Ring signature

All nodes are connected to the block header which is also called blockchain by storing the previous block TxID into the next block. When creating a new block, the blockchain will use consensus algorithm to create a unique identifier for a new transaction The consensus algorithm generates a new block which generates a new block by calculating the block header hash value. It'll be added to the blockchain after most nodes approve the new block.

2. METHODOLOGY

Convert Public key to Bitcoin address -

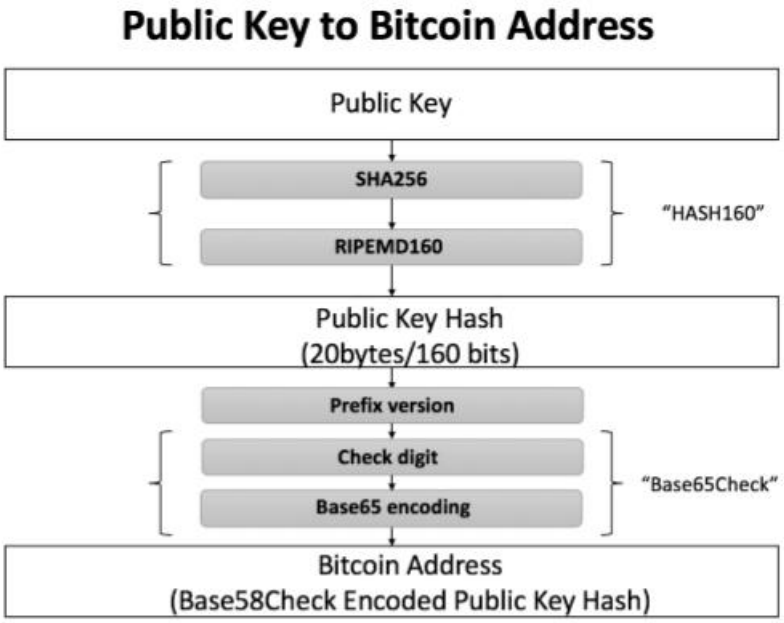

Fig.2.1 Public Key to Bitcoin Address

Generate the Digital Signature Algorithm Private Key by Elliptic Curve, commonly called secp256k1 The size of the private key on Bitcoin is 256 bits.

Generate the public Bitcoin key from the private Bitcoin key (x, y) using DER format.

Transform the public key of Bitcoin as PKhash160 into hash160 by generating the algorithm SHA256 and RIPEMD160

Apply the version prefix according to Table 2.1 at the head of PKhash160. Define the intermediate hash value for the fingerprint of the public key = prefix + PKhash160, which is also called the fingerprint.

Defines Sha256(Sha256(fingerprint)) as digit d of search. Apply d to fingerprint at the top.

Generate the final Bitcoin address by encoding the Base65 encoding algorithm with Fingerprint + d. Defines address = Base65(fingerprint+d) as the Bitcoin address ending.

2.1 CRYPTOGRAPHY

2.1.1 RSA ALGORITHM

RSA is a kind of cryptographic algorithm asymmetric algorithm used to encrypt and decrypt messages[29]. Its protection is based on the complexity of the decomposition of large integers. And there are a number of implementations. Might define the particular algorithm as follows.

1.Select two large prime numbers of different sizes.

2. Let n = pq, f(n) = (p−1)(q−1).

3. Select e [0,π(n)−1].

4. Calculate the modular reverse multiplicative of F(n) as d that ensures ed = 1 mod f(n).

5 Defines e, n as its public key and p, q, d as its private key

6 Encryption: Enter x, compute y = xd mod n to encrypt the message using the public key (e, n).

Decryption: send y, calculate x = yd mod n to encrypt the message using the private key (p, q, d).

2.1.2 RING SIGNATURE

In 2001, Rivest, Shamir and Tauman raised a question as to whether the code could be leaked[28]. They told a story about a cabinet member revealing details against Prime Minister to address this issue. Bob is a cabinet member who wants to send a letter to the journalist about the Prime Minister's illegal activities. Bob must notify him of an secret channel to ensure his health, and then the journalist can easily verify his cabinet identity.

Bob cannot use a group signature scheme to send the message to solve this issue, since he can't confirm that the group administrator is managed by the prime minister. They suggested a new scheme called a ring signature, where each cabinet member is the ring leader and everyone is equal and anonymous. One may define the ring signature scheme as follows. Suppose there are a total of n participants of the scheme. He has his own public key yi and his private key xi for each user Ui, and they sit in a ring as Figure 2.2. The scheme can be divided into three parts: a main pair is generated, a ring signature is generated and the signature checked.

Making a key pair: A key pair generator algorithm for the signer by computing the symmetric key ki. The algorithm will measure the ki for any public key yi and private key xi.

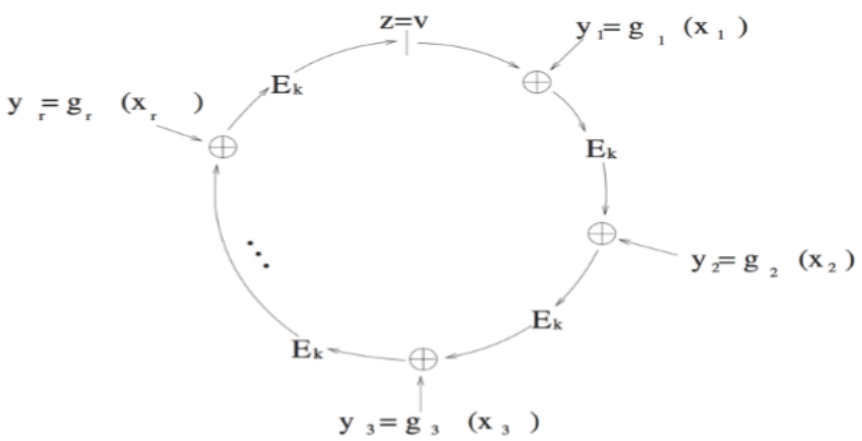

Fig 2.2 Ring Signature

Generating a ring signature: by entering the signer's message m, n numbers and its public key list L = y1,y2,y3, .. ,yn and the signer's private key xi, the algorithm will produce a signature called the ring signature as π. Signature verification: Inputting message m and ring signature π. If λ is m's signature, the output is true and the other output is false. The security properties and advantages for the ring signature can be divided as anonymity and unforgeability

1. Unqualified anonymity, Even if the intruder takes all the voters' private keys, the probability of verifying the voter's identity would be less than 1/n, which is n numbers of all participants in the ring.

Unforgiving, Even if the outside intruder tampers a ring signature according to message m without any of the voters' private keys, the chance of coincidence may be ignored.

Compared with the group signature scheme, the ring signature scheme does not have an administrator in the group. Every member is equal and no trusted third party is required on the scheme.

3. PROTOCOL

3.1 DESCRIPTION

The proposed protocol shall consist of three entities: the Voters (Vi), RA (Registration Authority), EA (Election Authority) and Bitcoin Address Pool. Voters (Vi): Elections should be a list package. May be specified as Vi for every voter to vote. Candidate(Ci): The nominees should be a list selection. That can be described as Ci for every candidate to vote. Registration Authority(RA): Initially, the voters will register as a register in the new e-voting system. Voters will store their public keys(PKi) and Bitcoin address(Ai) in this program, and move it to the database via the program. For the RA it provides voters with the candidate(Ci).

Electoral Authority(EA): The electoral authority is responsible for the collection of votes. The EA has its own address Bitcoin(AE). After the vote is over, the EA will start counting the votes and pass the result to the voting system.

Bitcoin Address Pool: The Bitcoin Address Pool is a list of all randomly generated Bitcoin Addresses from the EA network using ECC algorithm. Each address's private key SKAi will be stored into the EA system.

Public oversight: Some of the content should be available and monitored as the open-audit component for everyone to create this protocol. The completeness and validity can be verified by anyone.

3.2 PROTOCOL

3.2.1 OUTLINE

The entire creation of the Protocol shall consist of seven sequential steps, each of which shall be carried out by separate actors.

Preparation Phase: The Election Authority (EA) will initially set up a new voting project and then store the address of Bitcoin as its private key in the EA program.

First Registration Phase: Nearby residential areas are located the voting registration stations operated by Registration Authority (RA). Voters and candidates for election are entitled to vote upon passport authentication or other necessary IDs. Participants will be sent a random register code via email as a connection by RA.

Second Registration Phase: Using key pair tools or local RSA tool, participants can generate their public key and private key by clicking on the RA-sent random register code connection. The new created public key should be stored in the system while private key should be kept private.

Publish Phase: Every single public key from the voters will be obtained under supervision at the vote cut-off date. As long as you click on the start vote button, RA will no longer allow new registration requests.

Voting Phase: When voters use their private key to sign preferred candidates, they will receive a unique ring signature that is transmitted to the blockchain.

Tallying Phase: The tallying stage is strictly monitored by the public, people can access the tally page to see or cast ballots. Verification Phase: On blockchain, EA transaction history is available to the public to track the validity of the vote result.

3.2.2 ASSUMPTIONS

The protocol shall be based on the assumptions to encourage privacy and verifiability properties.

1. It does not comply with the registration authority and the electoral authority.

2. Sha256) (is a stable hashing algorithm.

3. Every actor follows the phases of enrolling the voting case.

Now we're going to explain the phases we've been thinking about earlier.

3.2.3 PREPARATION PHASE

The specifics of this process may be defined in the following order.

The EA is storing its own Bitcoin(SKb) private key into the network.

The machine will generate Bitcoin address (AEA) of the EA from its Bitcoin(SKb) private key.

The EA generates a new voting item with the voting id(Li), title, restriction of the number(s) of votes and the definition of this voting item.

The EA program will automatically produce the numbers for the n bitcoin addresses(A1,A2 ... An) as the Bitcoin Address Pool

3.2.4 FIRST REGISTRATION PHASE

The specifics of this step can be defined in the following order.

1. The candidate(Ci) directly takes his / her passport and authenticates to the RA.

2. The RA verifies the candidate's identity and asks for his name, personal description, and saves it into the RA program.

3. The RA will create his candidate id(Ci) and give him the I d.

4. The voter(Vi) directly takes their passport and authenticates to the RA.

5. The RA verifies the voter's identity and asks for the voter's email address, then sends him an email with a random code connection as LKi to prevent multiple registrations.

6. The LKi is generated at random and has no connection with the voter's name and email address

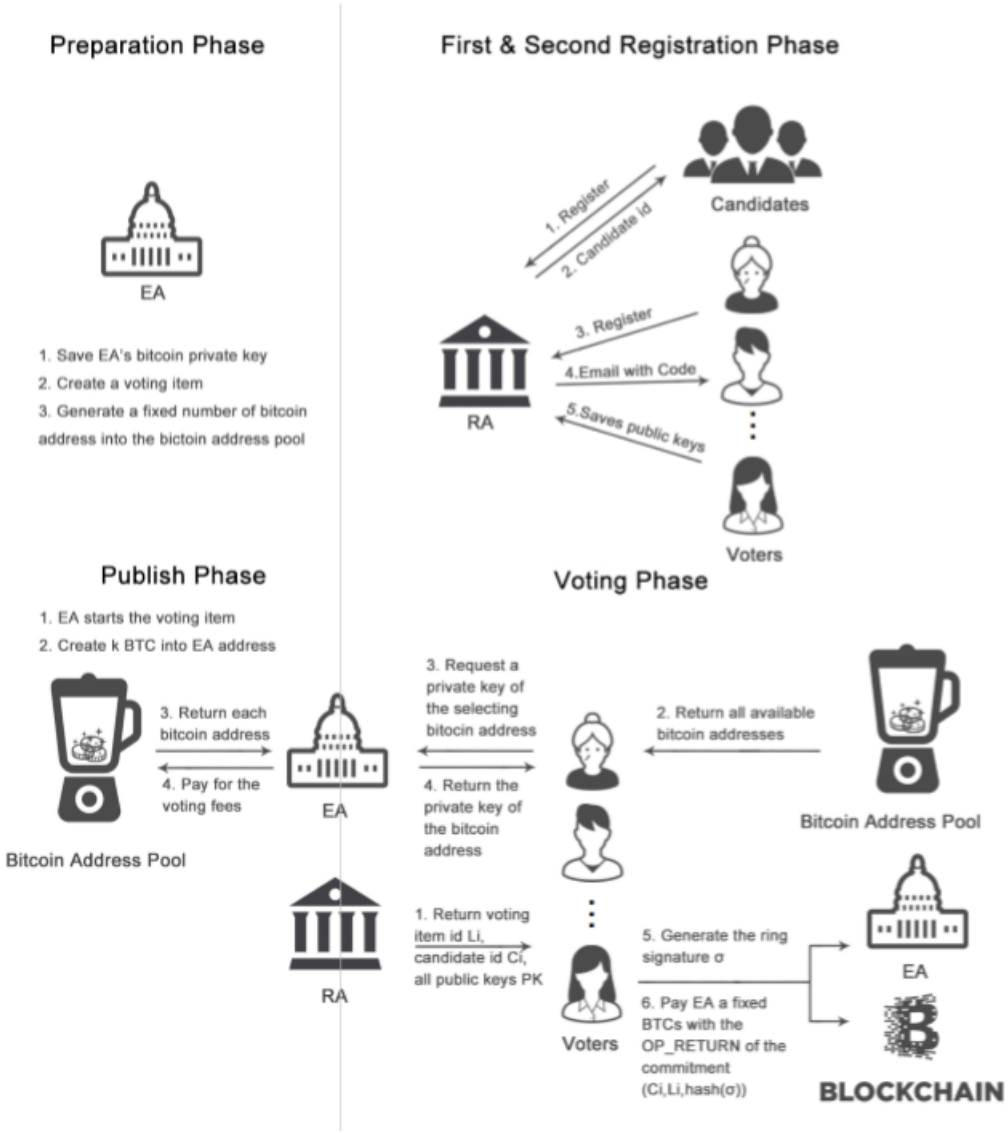

Fig 3.1 Proposed Protocol(Mainly Phases)

3.2.5 SECOND STAGE OF REGISTRATION

The specifics of this step can be listed in the following order.

1. The voter opens the LKi Logging Connections.

2. Voting Vi generates the main pair (SKi, PKi).

3. Voting Vi saves the PKi public key into the network.

4. The collection of voters should be defined as a number n at the end of the registration.

3.2.6 PUBLISHING PHASE

The specifics of this process may be defined in the following order.

1. The EA agrees to start voting on the cut-off date which means the ring of public keys has been confirmed and the RA does not consider any requests for registration.

2. EA builds its own Bitcoin wallet with k BTC.

3. EA charges for every Ai a fixed sum of bitcoin k / n as the voting fees, such as 0.0001 BTC. (Upon voting, the voting fees will be returned to EA).

3.2.7 TALLYING PHASE

The details of the phase is described as follows.

1. The system returns all sets of (σ,sha256(σ)) and all public keys PK automatically.

2. The system fetches all transactions in EA Bitcoin address AEA automatically

3. The program fetches each transaction from the OP RETURN and verifies the validity of the signature ÿ.

4. The system counts every transaction that is legitimate and adds 1 to candidate Ci.

5. If voters Vi are absent, mark them as abstaining from voting.

6. If the history of the Bitcoin transaction has transactions from the same Ai more than twice, count the first one and ignore others.

7. Verification Step

3.2.8 VERIFICATION PHASE

The specifics of this process can be defined in the following order.

1. The program immediately returns all Public Keys (PK1,PK2,PK3 ... PKn).

2. He will use a set of all public keys (PK1,PK2,PK3 ... PKn), the ring signature π, the candidate Ci to check his vote for each voter Vi.

3. Voter Vi will use the transaction ID to get the blockchain's commitment to check if the signature is being released in the correct way.

4. EVALUATION

4.1 EXPECTED PROPERTIES

The properties of the voting scheme are necessary, in accordance with the properties mentioned above. The properties can be described as below, for this protocol and implementation.

Security ballot: No-one knows on whom the elector voted. The address of the blockchain account is random, and no external observer or even the program is unable to know the relationship between the voters and the Bitcoin address. It has its own property of anonymity for ring signature. No one may infer the elector's true identity from the ring signature.

Individual verifiability: After voting, the voter can verify that his ballot is correctly counted. To check that the sha256(π) is published correctly to the blockchain, where π is the signature, the user will use the (π,sha256(ÿ)). The elector will use his ring signature to check that he is voting for the correct candidate.

Eligibility: The voting case can only be registered by the valid vote. Under this method, if the voter is checked to be legal to vote, the voter will register under RA, and get the code connection. Once voting starts, the voting event can only be enrolled by the voter who has the code connection.

Completeness: Every vote should be correctly counted.

All votes can be correctly counted. The program will include all public keys through the use of ring signature. When the vote is over, the EA blockchain account will earn an sum of bitcoins. The tallying method will easily count the per transaction's OP RETURN. Anyone who refuses to vote but saves his PKi public key to the program would be considered abstention.

Uniqueness: Every elector will vote only once. When he votes, the candidate won't get permission to vote more. The protocol has a system whereby extra votes from the same voter are ignored. In the tallying process, if the past of the Bitcoin transaction has transactions from the same Ai more than twice, count the first and ignore others.

Robustness: When tallying, someone can't manipulate or change the final outcome of the vote. When the elector votes, the result was broadcasted to the blockchain. The blockchain is difficult to forge and to alter.

Coercion-Resistance: No coercer should work with the voter. The voter cannot say who he was voting for. The protocol will ensure this property only occurs when the number of voters n is sufficiently increasing. If someone threatens a voter to vote for him, a transaction I d and the ring signature that vote for the public API threat can be given to the voter. For the hazard, the signature voter cannot confirm that he belongs to the voter. The tallying system gathers all Blockchain account address transactions from EA. The method verifies the legitimacy of the ring signature when counting the votes, and records only the first and legitimate vote.

With this protocol and implementation not all properties are fulfilled. Here are the properties which the implementation does not satisfy.

Fairness: None of this will affect the vote outcome. In real time, the tallying mechanism is in. The property cannot be guaranteed by the program.

Receipt-freeness: Upon voting, the elector cannot obtain or attempt to create any receipt to show how he votes. Once the user starts voting, he gets the blockchain's ring signature ÿ, sha256(π) and transaction ID. It is the voter's receipt to validate his ballot.

5. CONCLUSION

5.1 DESCRIPTION

This paper primarily discussed the basic principle of e-voting and blockchain by defining the Bitcoin address algorithm and the principle of OP RETURN.

A seven-phase, blockchain-based protocol was later introduced. Specific step description and method were clarified in depth as well.

The entire process of protocol creation was also defined from the perspective of transitional software development, such as how the blockchain transaction occurs, and some voting system function research.

Finally, the paper discusses the protocol's performance and possible safety risks, and further drawbacks were addressed at the end.

5.2 SUMMARY

Since the protocol created satisfies the ballot-privacy properties, person verifiability, competence, completeness, uniqueness, robustness and coercion-resistance. It does not satisfy justice and receipt-freeness requirements, however.

The protocol works efficiently for ring signature in the performance assessment, particularly when the voter number is less than 3000. Therefore ring signature algorithm efficiency is constrained by the number of participants. The principal benefit of this system is to guarantee electronic voting validity.

As every vote is broadcast to the blockchain until voting begins. Moreover, since blockchain is a decentralized distributed ledger, the outcome of the ballots is represented in real time and cannot be changed by an entity, which satisfies the open-auditing concept.

The aim of selecting test-net as the blockchain network, primarily in comparison with Bitcoin and Ethereum, lies in its free and easy way. In addition, the high degree of similarity to the structure of the Bitcoin network is another big justification for nominating test-net to broadcast the outcome of the vote.

REFERENCES

[1] Baudron, O., Fouque, P.-A., Pointcheval, D., Stern, J., and Poupard, G. Practical multi-candidate election system. In Proceedings of the twentieth annual ACM symposium on Principles of distributed computing (2001), ACM, pp. 274–283.

[2] Benaloh, J., and Tuinstra, D. Receipt-free secret-ballot elections. In Proceedings of the twenty-sixth annual ACM symposium on Theory of computing (1994), ACM, pp. 544–553.

[3] Bitcoin-Wiki. Confifirmation - bitcoin wiki. https://en.bitcoin.it/wiki/Confirmation.

[4] bitcoinfees.21.co. Predicting bitcoin fees for transactions. https://bitcoinfees. 21.co/.

[5] Card, D., and Moretti, E. Does voting technology affffect election outcomes? touchscreen voting and the 2004 presidential election. The Review of Economics and Statistics 89, 4 (2007), 660–673.

[6] Cetinkaya, O., and Cetinkaya, D. Towards secure e-elections in turkey: requirements and principles. In Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on (2007), IEEE, pp. 903–907.

[7] Chaum, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24, 2 (1981), 84–90.

[8] Christian Schaupp, L., and Carter, L. E-voting: from apathy to adoption. Journal of Enterprise Information Management 18, 5 (2005), 586–601.

[9] Cohen, J. D., and Fischer, M. J. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science, 1985.

[10] Cranor, L. F., and Cytron, R. K. Sensus: A security-conscious electronic polling system for the internet. In System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on (1997), vol. 3, IEEE, pp. 561–570.