Electronic Voting System Implementation Through Bitcoin Blockchain Technology

Cassandra Schultz
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA 56267
schu4276@morris.umn.edu

ABSTRACT

Even with all the advances we have seen in secure digital technology, the most secure way to currently cast a vote on election day consist of a hand-marked paper ballot. When extenuating circumstances arise, offering a voting environment that is accessible and safe for everyone, but also secure can be a difficult task under the current voting system. This paper discusses one proposed electronic voting system which uses blockchain technology. Based on a review of literature on blockchain technology and specific implementations of voting systems, a summary of relevant background information as well as implementation protocol are provided. Even though experts believe that societies are not currently ready to implement systems like the one described in this paper, the technology to create a secure and efficient system does exist, and could one day become available.

Keywords

Blockchain, E-Voting, Cryptography

1. INTRODUCTION

Voting in local and national elections mark one of the few chances the typical member of society has to express their democratic right and personal views. In the most recent national election (2020), 69.9% of registered voters were living in jurisdictions that use hand-marked paper ballots for the majority of voters [8]. This method of voting is used because it is able to offer *verifiability*, *uniqueness*, and *security.* [3].

These properties are invaluable, and without them, a voting system can not succeed. At the same time, there are challenges that may, and often do arise at a national, regional, and individual level that deem hand-marked paper ballots as inaccessible, unusable, or inefficient. These challenges broach the subject of an electronic voting system (e-voting).

With this challenge in mind, Stefano Bistarelli, Ivan Mercanti, Paolo Santancini, and Francesco Santin proposed an e-voting system that leverages technology currently being utilized for Bitcoin [3]. The researchers describe an innovative implementation of a potential system with more decentralization, and accessibility than the current voting system is able to offer. More importantly though, the proposed voting system meets the same security, integrity, and verifiability properties that validate the hand-marked paper ballot system [3].

The proposed implementation is entirely based on existing blockchain technology as implemented by Bitcoin. Verified voters are each given their own virtual *wallet.* The researchers use the term wallet to refer to an individual's voting wallet on their personal computer, or a web portal which assists with the vote casting processes. The wallet is part of the web application they call 'Coin Prism' [3]. This implementation offers verifiability and security from the point of candidate nomination to the release of election results.

The results of the proposed blockchain system were promising. The researchers were able to effectively meet all the standards of a functional voting system. The implications of this proposed technology could increase voter turnout by making voting more accessible to those who may not be able to vote in person, or even just easier for those who would prefer not to vote in person [7]. The decentralized nature of the blockchain could also offer efficient and accurate audits and recounts.

In this paper, I first introduce some background information about a few major relevant cryptographic concepts. I will then introduce, and discuss the aforementioned electronic voting system in 3 phases. Section 3.1 will discuss the pre-voting phase, section 3.2 will discuss the voting phase, and section 3.3 will cover the post-voting phase.

2. BACKGROUND

There are a few major requirements that are expected to be met by any successful voting system. This section will briefly define those requirements in the context of electronic voting. Furthermore, this section includes a bit of information about what our current voting systems do to meet those requirements.

2.1 Verifiability

In this context, verifiability means that there must be a practical way to verify that all votes have been accurately accounted for and correctly counted. This also means there must be a reliable collection of election records that include details about the authentication and voting process. Paper voting systems meet these requirements easily, as all the votes are physically stored, and available to refer back to should the need arise. Meeting the requirements of verifiability also means that records must be accessible, and usable in the case of an audit. For paper voting systems, this prop-

UMM CSci Senior Seminar Conference, April 2021 Morris, MN.

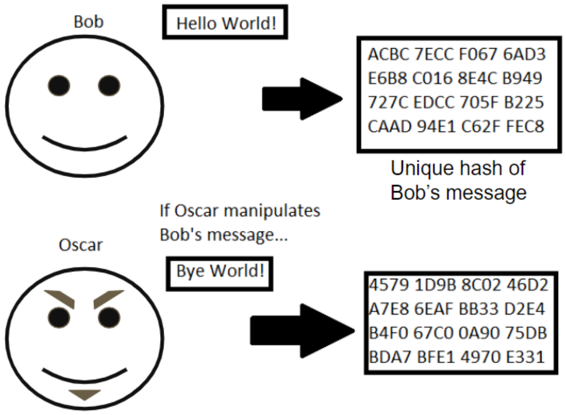

Figure 1: Secure Hash Function In Action [2]

erty is sometimes fulfilled with the help of poll workers who use either paper records, or *electronic poll-books*. These poll books are a computer-based system that poll workers use to look up registered voters in order to either check them in, verify the person's identity, or verify that the person is ineligible to vote. [8].

2.2 Uniqueness

Assuring that no individual can vote more than once is essential to an honest and democratic election. Electronic poll-books (see section 2.1) help to ensure uniqueness in the voting systems implemented today. [8]. Once an individual has cast a vote, the poll worker will update the voter's registration file to record that a vote has been cast. Any vote received by this same individual after this point will be denied. The same goes for those who mail in a vote as well as voting in person on the day of the election. Strict rules about voter registration also help to ensure that each person may only cast one vote.

2.3 Security

Furthermore, there must be a way to verify that each vote has not been tampered with at any point in the process. In paper voting systems, this property is achievable through the guidelines placed on the marking of ballots. These guidelines include things such as the nullification of ballots which contain improperly or ambiguously marked information. Mindful and secure storage practices of the paper records and poll books are also used to prevent manipulation of voter data. Another important part of voting security is the anonymity of voters. In order to avoid bias or coercion, it is crucial that a vote cannot be linked to the individual that cast it.

2.4 Cryptographically Secure Hash

Cryptographic hash functions are mathematical algorithms that map data of arbitrary size to a bit array of a fixed size. The bit array that results from a hash function may be referred to as the hash value. Hash functions are quickly computable, and impossible to invert. This means that there is no way in which the output of a hash function can be used to derive the input, such functions are referred to as *one-way functions*. Secure hash algorithms can be used to verify that the contents of a message have not been altered, note however this is different than encryption, as the function cannot be reversed. A simple example of this concept in practice may go something like this: *Alice* (a fictional character commonly used as a placeholder when discussing cryptographic systems and protocols) [2] wants to send a message through a public network, but when the message reaches its destination, Alice wants a way of knowing that her message has not been altered. In order to check the integrity of her message, Alice can create a hash of her message before sending, and after sending. If Alice compares these hashes and finds them to be the same, she will know the message is unchanged. This hash is essentially a unique ID for Alice's message, similar to a finger print, as it is very nearly impossible for two messages to yield the same hash value. Even the smallest change in a message, will result in a completely different hash, with no relation to the hash of the unchanged message.

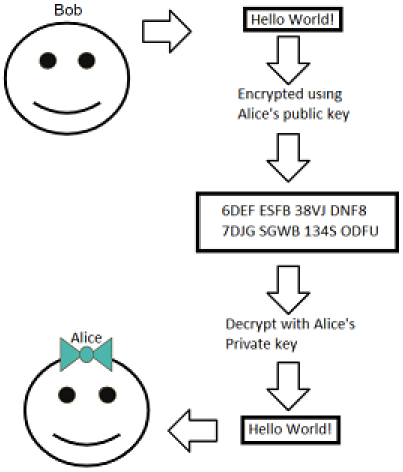

Figure 2: Asymmetric Cryptography [4]

2.5 Asymmetric Cryptography

Asymmetric cryptography, also referred to as public-key cryptography, is a cryptographic system that utilizes a pair of *keys* for each participant. In cryptography, a key refers to a group of characters in a particular order. These keys are used to specify the alteration of data so that it may be scrambled, or disguised such that anyone without the key will be mathematically unable to read the information. Keys are not intended to be read or remembered by humans, so most keys have low human readability. One of these keys is considered the *private key* and should be kept a secret. The second is a *public key* and should be made available publicly. A message that is encrypted using a public key, may only be decrypted with the corresponding private key. In the same vein, a message which is encrypted using a private key, may only be decrypted using the corresponding public key. This means that any individual has the ability to encrypt a message using their intended recipient's public key. When this encrypted message is sent, the sender knows only the owner of the corresponding private key will be able to read the message, and the wrong people will not (see Figure 2).

The security of asymmetric cryptography relies on the pri-

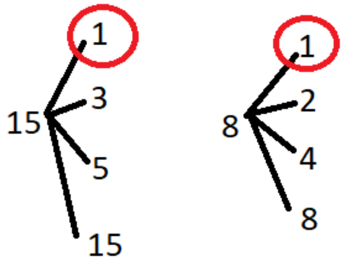

Figure 3: Since 1 is the greatest common divisor, these numbers are co-prime

vate key remaining private, and the public key being public knowledge. Keys can be generated in a number of different ways based on the algorithm being used, but the generation always involves the use of one-way functions (meaning functions which cannot be reversed).

2.6 Digital Signatures

A digital signature is a cryptographically secure mathematical scheme which employs asymmetric cryptography (see section 2.2) to verify the authenticity of digital documents and messages. This means that the receiver of the message is able to ensure that the message is from the person they expected it to be from and also that the message has not been changed anywhere in the process.

2.6.1 RSA Digital Signatures

One example of a digital signature scheme would be RSA digital signatures. The letters in RSA represent the initials of the three developers responsible for the algorithm, Rivest, Shamir, and Adleman. RSA digital signatures makes use of the *RSA Algorithm*, one of the more popular digital signature schemes [4]. There are other algorithms that may be used for completing digital signatures, but RSA is relatively straightforward, and for this reason, will be used to describe digital signatures in this paper.

2.6.2 Euler's Totient Function

Euler's Totient Function, denoted as $\phi(n)$ counts the positive integers, up to integer n that are co-prime (also called relatively prime) to n. Two integers a and b are called coprime if 1 is the greatest common divisor for a and b. $(15, 8)$ is an example of a co-prime integer pair, whereas $(10, 15)$ would not be a co-prime integer pair, because they are each dividable by 5 (see Figure 3). For further example, $\phi(6) = 2$, because in $\{1, 2, 3...6\}$, $\{1, 5\}$(a total of 2 numbers) are coprime to 6. An important property of Euler's Totient Function is that $\phi(p) = p-1$ where p is any prime number. This property will be leveraged in the digital signature process.

2.6.3 RSA Key Generation

The RSA digital signature scheme begins with the generation of a key pair. Key generation works as follows: two distinct large prime numbers p, and q are chosen, and kept secret. Large in this context means numbers with hundreds of digits. p and q are chosen randomly within a set of guidelines. After this calculation, n can be computed, as $n = pq$. This n will be used as a modulus for the key pairs later on. The next step involves calculating $\phi(n)$, *Euler's Totient Function*, as described above in section 2.6.2. Since we calculated earlier that $n = pq$, we can say $\phi(n) = (p-1)\times(q-1)$ this is possible because p and q are both prime numbers, and because Euler's phi function is multiplicative when the factors are relatively prime. This means that $\phi(ab) = \phi(a)\phi(b)$. Finally, e,*public key exponent*, and d, the *private key exponent* can be determined. e is chosen with the restriction that it must be within the range $(1, \phi(n))$, and e and $\phi(n)$ must be co-prime. d is simply calculated as follows: $e \times d = 1$ mod $\phi(n)$, this d is kept private along with p and q, while e and n are public. It is important to note that without knowing p and q, it is impossible to find d, even with knowledge of e and n.

2.6.4 Signing a Message

With the keys generated, a message can now be signed. If Alice wants to send a signed message to Bob, she must first produce a hash value of her intended message, and raise it to the power of d, (the private exponent). She then attaches this hash value raised by the private exponent to her message as a signature. The intention of a digital signature is not to disguise the contents of the message, but rather to confirm the source. Once Bob receives the signed message, he will raise the signature to the power of e (the public exponent). The reason he does this is to leverage the following equation: $h^{de} = h$ (mod n). Raising the hash value to the power of both the exponents yields the original hash value. With this, Bob can now compare the signature to the hash value of Alice's message, if the two match, he can confirm that the signature is valid and that the message came from Alice.

2.6.5 Blind Signatures

A blind signature is a special form of a digital signature, which disguises the contents of a message from the signer. This allows signing authorities to authorize digital documents without being aware of the contents of the message. Before a message is sent to the signer, the message is *blinded*, meaning the content is hidden in a way that can not be recognized by the signer. A real-world analogy to this procedure would be handing a completed ballot to a voting official in a sealed carbon paper envelope which has the voter's credentials written on the front. The official signs the ballot through the envelope via the carbon paper and the voter is now free to cast their ballot how they choose, and the authenticity may be verified via the official's signature. [4]

One way blind signatures may be implemented is with RSA blind signatures. This process begins with the Alice multiplying the message m by what is called a *blinding factor*. The blinding factor is a random number r raised to the power of e, similar to the digital signature procedure discussed in section 3.1.3. Alice then sends this blinded message (m', where $m' = mr^e$) to a signing authority. Because the blinding factor is both random and very large, the signing authority will have no way of reading the message they are signing. After adding a digital signature, the blinded and singed message s' is sent back to Alice as $s' = (m')^d$. Alice now needs to unblind the message. To remove the blinding factor, Alice can multiply the blind signature by the inverse of the random integer r.

$$\begin{aligned} s &= s' * r^{-1} \\ &= m^d * r^{ed} * r^{-1} \\ &= m^d * r * r^{-1} \\ &= m^d \end{aligned}$$

This leaves Alice with a valid digital signature on her original unblinded message

3. BLOCKCHAIN/BITCOIN

Blockchain is a chain of digital blocks that can hold information. This framework was originally created to implement and utilize digital timestamps for important documents to prevent tampering. Now though, it is the basis of the popular digital crypto-currency Bitcoin. More specifically a blockchain is a *distributed ledger* or a special type of database which is shared and replicated in a synchronized manner across all the members of a decentralized network [6]. Unlike many other databases, once a piece of data is added to the blockchain, it is very difficult to remove.

Each individual block contains data, the hash of the block, and the hash of the previous block. These hashes, as described in section 2.1, are like a unique finger print that depends on the entire contents of the block, including transaction details in the case of Bitcoin. Storing the previous block's hash acts as a security measure to protect the blockchain from undetected changes. If a block is compromised or manipulated, the hash of that block will immediately change, and as a result, it will not match the hash that is stored in the subsequent block. This makes manipulation of a block chain extremely difficult, in order to manipulate one block in a chain undetected, you would have to alter every other block that follows it.

3.1 Proof-of-work

Proof-of-work is a piece of data that is difficult to produce, but easy to verify, and is the mechanism which slows down the creation of new blocks. For Bitcoin, the proof-of-work aims to make the work of 'mining' (adding a block to the blockchain through valid hash generation) very energy-intensive, and somewhat time-consuming. In order for a new block to be accepted into the network of participants, the miner must create a block in which the hash of the block's header is lower than or equal to the current *target*. This target is a 256-bit number (a *very* large number) that all Bitcoin clients share. While the target number is large, it is only a very small percentage of the total options of possible numbers. The difficulty of the proof-of-work can be adjusted by lowering, or raising the target number. Bitcoin adjusts the difficulty to limit the rate of new block generation to one per every ten minutes [1].

3.2 P2P Networks

Peer-to-peer network $P2P$ is a decentralized network communication model that consists of many devices (or *nodes*). Each of the nodes collectively stores and shares files without any sort of centralized server or administration. This allows for a network where no single node is more powerful than any other node. In terms of blockchain architecture, this property allows for anyone to participate in the process of verifying and validating a new node. The transactions of the blockchain are stored on each node of the network, and together these devices are able to reach and keep a consensus on the accuracy of the data at all times. This also means greater security and stability should one of the nodes crash or go down. There are plenty of other nodes available, thus no one is able to take down the blockchain in this manner.

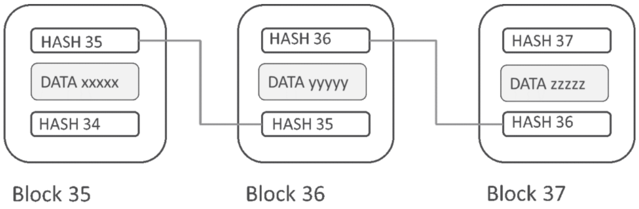

Figure 4: Chain Diagram

4. USING BITCOIN BLOCKCHAIN FOR E-VOTING

The researchers behind the following E-voting implementation decided that the process would be best organized by dividing it into three stages, pre-voting, voting, and the counting phase. Each of these stages works together to create a voting system that meets all the requirements as discussed in section 2.

4.1 Pre-voting Phase

4.1.1 Candidate Nomination

The first set of the pre-voting phase consists of voter registration. It is recommended that this process remains quite similar to the process that is required of voters now. At the time of voter registration, a system in which candidates can be nominated is created and implemented. Furthermore, there must be a means for the candidates to be eligible to receive votes. As for this implementation, the researchers decided that each candidate is given a part of asymmetric keys, one of which being public, and the remaining key is private. The candidate's public key is made available to all voters. For security, and to reduce that chance of manipulation, these keys would not be available on a government web page, but rather they would be provided to the voter at the time of voting.

4.1.2 Voter Authentication

The blind signature protocol, (as described in section 2.6.5) in this case takes place between the Authentication Server (AS), and the voter. The Authentication Server is responsible solely for authenticating the identity of a voter, and nothing else. The voter will be required to provide a form of official identification, likely an ID, or another document of this nature. Along with this identifying information, the voter will send their blinded public key to the Authentication Server for signing. The Authentication Service will receive the blinded public key along with the information proving the voter is who they claim to be. For the sake of voter anonymity, it is very important that this process is be completed via a blind signature. This means that the Authentication Server will have no way of connecting the voter's public key, to their physical identity, and thus have

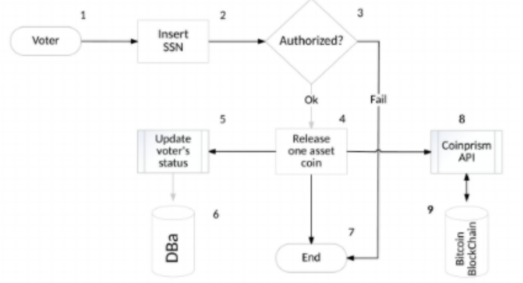

Figure 5: Visual Representation of Pre-Voting Phase [3]

no way of connecting a vote to a specific individual. Immediately following the blind signing, the signed key is returned back to the voter, who can unblind the key and the signature. With this, the voter has a signed and authenticated public key.

4.1.3 Token Distribution

Token distribution is the second phase of the voter authentication process. The Token Distribution Server is a completely separate entity from the the Authentication Server. This is an important strategic decision that helps to protect voter identity. The role of the Token Distribution Server is to distribute tokens to voter's who have a public key which has already been signed by the Authentication Server (Section 4.1.2). A voter will send their signed key unblinded to the Token Distribution Server, who has no knowledge of the voter's identify. The server simply knows that their identity has been authenticated, and that they are ready to receive a voting token via their public key. This voting token is essentially like a coin with which a vote may be cast. To cast their vote, a voter will transfer this coin to the candidate of their choice.

4.2 Voting Phase

Once the voter has been authenticated, and the candidates have been nominated for candidacy, the voting phase is ready to commence. This stage involved the preparation, and transfer of the voting token to the voter's candidate/party of choice, and confirmation of the vote's transmission. All of their operations can take place via the voter's wallet. Self-checking for the party/candidate's revival of the vote is as easy as checking to see if the transaction is present in the blockchain. The vote may be cast by the user via a simple web browser [3]. Through the web interface, the voter chooses a candidate via a database and casts their vote via their web-based wallet (the wallet is not presented to the user directly, and rather this is hidden behind a more user-friendly transaction process). After their vote has been cast, the voter is given a transaction ID. This ID is their receipt, which they can use to check on the status of their vote. Through this, they will be able to see if their vote has been assigned as they intended.

4.3 Implementation

Now that Alice has her token, she may transfer her token to the candidate she likes using an online console. The designers of the system offered up a design for this console that looks like the picture in figure 6. Alice transfers her token to the address of her preferred candidate. This vote can be authenticated as a valid vote on arrival by checking the validity of the attached digital signatures, if the token has a signature from the Authentication Server, the token can be accepted. Alice can confirm that her vote has been counted by checking if her vote has been added to the blockchain. To send the token to her candidate, Alice uses her private key to sign a message with the information about the transaction including information about the source of the voting token, and information about the destination address. The vote is then broadcast to the peer-to-peer network, where consensus among the chain can be confirmed. The vote will then be added to the chain permanently, where it can be refereed back to should the need arise.

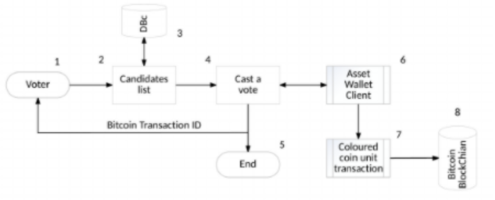

Figure 6: Visual Representation of Voting Phase [3]

4.4 Post-Voting Phase

The post-voting phase involves the counting of votes, and also addresses concerns such as recounts, and the audit of votes.

4.4.1 Counting Votes

After the end of the voting-phase, the cast votes may be counted by taking the sum of the tokens received by each candidate/party. The counting process sums only the transactions which are deemed valid by two major criteria. The first of these being that the transaction originates from an authorized voter and the same transaction moves immediately to and ends at the address of a validly nominated candidate. The relevant information to make this check is stored in detail within the blockchain. Specifically, only legitimately received tokens will be counted(section 4.1).

Because the blockchain keeps permanent record of the source addresses for all confirmed votes, this can be used to confirm that only one vote per authorized voter is counted, if more than one vote originates from the same public key address, only the first valid vote will be counted.

5. PRACTICAL CONSIDERATIONS

5.1 Voting System Requirements

The potential success for this voting system can be evaluated by observing the requirements for a successful voting system, and analyzing how and if these basic needs were met by the protocol described above.

To maintain uniqueness, voters are restricted to voting only once because double spending is not a possibility with the blockchain technology used by Bitcoin. This system also maintains voter anonymity, by completely separating the Token Distribution Service and the Authorization Service, the anonymity of each vote can be safely ensured. Furthermore, it is important that only those who have legally registered voters take place in the voting process. This requirement is also filled through the pre-voting phase as described above (section 4.1). Beyond these security measures, it is important that the voting system is verifiable (section 2). This system meets this requirement by ensuring that votes are not just accurately countable once, but are accurately able to be recounted, and audited with reasonable ease. This is achieved in the implementation described through the permanent storage of the blockchain. A vote 'transaction' is stored permanently, and the hash of the last block of an election may serve as evidence should the question of tampering come up. The fact that every node contains a copy of the blockchain also means that recounts and audits can be verified with strong consensus.

6. CONCLUSION

Electronic voting, and specifically internet voting systems are facing a lot of opposition from experts in the field. The Verified Voting Foundation, a foundation that works to equip election officials with the tools they need to validate election results, and also helps to move states towards the best election security practices. The Verified Voting website (verifiedvoting.org) includes an entire page warning about the dangers they see in internet voting. They express concerns about the ability of foreign state actors who may want to meddle with the results of an election. Their main concern is the lack of a voter-verified paper record. Their other main concern relates to the lack of privacy for voters. Because these things are not offered in any currently offered or implemented electronic voting system, voting with hand-marked paper ballots is the safest and most secure system.

A system such as the one described above has not yet been implemented on a large scale, but there are a number of countries that have tried to implement different forms of electronic voting. Africa in particular, conducted a substantial amount of social sciences research as it relates to electronic voting. The research revealed some similar concerns to those described above from the Verified Voting Foundation. One of the major concerns for remote electronic voting that emerged in this study was the increase in concern for vote-buying and coercion, two things that voting in person on a hand-marked ballot can effectively prevent. These are concerns that were not described in this paper and are concerns that would need to be addressed before the system could be implemented [5].

Acknowledgments

I would like to thank Dr. Elena Machkasova, and Nathan Beneke for their advice, feedback, and dedication to helping with my work. I would also like to thank Grace Randolph, and Beth Nemec for all their love and support throughout the process.

7. REFERENCES

[1] Bitcoin wiki. [Online; accessed 17-Feburary-2020; https://en.bitcoin.it/].

[2] Cryptography wikipedia, Jan 2021. [Online; https://en.wikipedia.org/wiki/Cryptography].

[3] M. Bistarelli and S. Santancini. End-to-end voting with non-permissioned and permissioned ledgers. *Journal of grid computing*, March 2019.

[4] G. Bleumer. *Blind Signature*. Springer US, Boston, MA, 2011.

[5] A.-M. Oostveen and P. V. d. Besselaar. The academic debate on electronic voting in a socio-political context. Oct 2019.

[6] B. P. Sloane Brakeville. Blockchain basics: Introduction to distributed ledgers. June 2018.

[7] K. Stewart. Online voting: The solution to declining political engagement?, Mar 2018.

[8] VerifiedVoting. Polling place equitment—VerifiedVoting, 2020. [Online; accessed 17-Feburary-2020; https://verifiedvoting.org/verifier].