Chapter 1

abstract

Chapter 2

Introduction

> "These are revolutionary times. All over the globe men are revolting against old systems of exploitation and oppression, and out of the wombs of a frail world, new systems of justice and equality are being born." -Martin Luther King, Jr.

We are forced to make decisions every day. Some decisions are simple. What do I eat for dinner? What do I wear today? Other decisions are more difficult. What politician should I vote for? Which stocks should I invest in? This decision making process is complicated, and becomes even more so when we try to make decisions as a group.

All organizations have power structures through which decisions are made. Democratic societies aim to make decisions by granting and counting individuals' votes. This process is complicated in practice, but in theory helps to provide a fairer and more balanced society. Unfortunately, the difficulties of actually implementing such a system can lead to imbalances, fraud, and corruption. Gerrymandering, vote buying, and private interests are real-world examples of the shortcomings a democratic society might incur.

The growing usage and near-ubiquitous nature of the internet and personal computers offers a new medium through which a vote could be cast. Online voting might offer solutions to alleviate some of the shortcomings previous demo-

cratic institutions have been victim to. However, online voting has been shown to have many of its own risks associated with it.

Here online voting, its feasibility, scalability, security, and potential implementations are explored. In particular, blockchain technologies are considered as a means to address some of the issues and risks that have been shown to exist in other voting systems. Ultimately, could a transactional, decentralized, secure, verifiable, and electronic voting system exist?

Chapter 3

Background

3.1 Governance

A **government** is the means through which a community is managed. Governments might be best grouped by three attributes: those in power, how decisions are made, and the distribution of responsibility among those in power.

Those in power:

Term	**Definition**
Kraterocracy	Rule by the strong, "might makes right".
Plutocracy	Rule by the wealthy.
Geniocracy	Rule by the intelligent.
Meritocracy	Rule by the meritorious.
Technocracy	Rule by experts.
Timocracy	Rule by the honourable.
Autocracy	Rule by a single individual.
Oligarchy	Rule by a small group of powerful individuals.
Monarchy	Rule by family.
Democracy	Rule by the people, enfranchized citizens.
Anarchy	Rule by none.

https://en.wikipedia.org/wiki/Forms_of_government#By_elements_of_where_decision-making_power_is_held

How decisions are made:

Term	Definition
Demarchy	Decisions are made by randomly selected citizens a pool of enfranchised citizens (sortition).
Direct Democracy	Decisions are made by citizens vote on policies directly.
Representative democracy	Decisions are made by representatives elected by enfranchised citizens.
Liberal democracy	A form of representative democracy that attempts which operates under the ideals of liberalism.
Social democracy	A socio-economic democracy which supports economic and social intervention within the framework of a capitalist society.
Electocracy	Decisions are entirely made by a government elected by citizens.
Totalitarian democracy	Decisions are made entirely by representatives elected by citizens.
Constitutional monarchy	A monarchy where the monarch's powers are limited by a constitution.
Crowned republic	A republic with a ceremonial monarchy.
Absolute monarchy	Rule by family.

Distribution of power lies mostly along a single axis from democracy to autocracy. Between there usually exists some level of federation which governments operate under.

3.2 Voting

If we exclude singular autocratic and chaotic anarchic forms of governance then a system usually arises where voting is necessary.

Voting is a means to come to consensus as a group; the goal of which should be reaching a consensus which reflects the preferences of the participating actors in the fairest way possible. Voting, at first glance, seems like a trivial problem, and perhaps is under most inconsequential circumstances (a small group of actors with limited choices). However, voting quickly becomes a difficult problem once the number of actors or choices increases. There are mathematical constraints that voting systems are bound by. Beyond mathematical constraints there are challenging social and engineering issues with which an implemented voting system will be subject to.

3.2.1 Systems

A **voting system** is the combination of rules which define how a final result, and ultimately consensus, will be determined during a vote. All voting systems are composed of three important pieces: ballot, choices, and tallying method.

3.2.1.1 Choices

A voting system's **choices**, or **options**, are the set of choices that a voting actor can select from; they are the *who* or *what* being decided in a vote. The choices available may be determined by primary vote, polling, write-in, or some combination of techniques.

3.2.1.1.1 Representative Democracy

In a **representative democracy**, choices are candidates who are meant to represent their constituents. A **republic** is an example of a representative democracy.

3.2.1.1.1.1 Indirect Election

An **indirect election** is a vote where actors vote for persons who then elect a candidate themselves. The electoral college used in the United States is an example of this. When voting actors cast their vote for a particular candidate they're actually voting for **electors**, members of the electoral college who are typically aligned with the candidate's party. These electors are expected to vote for the candidate who wins the majority vote in a their state. In all but two states the electors are "winner-take-all", that is, if a candidate wins the popular vote in a state, e.g., by 50.1%, then all of the electors selected for that state will be electors aligned with the winning candidate.

3.2.1.1.1.2 Direct Election

A **direct election**, in contrast to an indirect election, is a vote where a voting actor's votes are cast directly for a candidate.

3.2.1.2 Ballot

A **ballot** is the means through which voting actors express their vote. The structure of the ballot influences exactly *how* the voter can express their preferences for a choice or choices. This is directly influenced by the tallying method. Ballots, in some texts, are regarded to as a *process* of voting; here we use it to describe the medium through which a voting actor marks their choice (e.g., paper, punch card, or electronic machine), and the rules regarding how they can mark said medium.

3.2.1.3 Tallying Method

3.2.1.3.1 Plurality Voting

A **plurality vote** is one where

3.2.1.3.2 Ranked Voting

A **ranked vote** is a

3.2.1.3.3 Unweighted votes

3.2.1.4 Conclusion

The choices affect *who/what* you vote for, the ballot affects *how* you express your vote, and the tallying method affects

3.2.2 Theory

Voting theory, also known as **social choice theory**, is the mathematical study of voting systems. Voting theory is used as a tool to examine voting systems, their caveats, and their benefits. As it turns out, there are lots of interesting and often unexpected results that can occur depending on the voting system being used.

3.2.2.1 Arrow's Impossibility Theorem

When considering governance and voting Arrow's impossibility theorem is a good place to start, it grounds one to the difficulties of voting. Arrow's impossibility theorem states:

> When voters have three or more distinct alternatives (options), no ranked order voting system can convert the ranked preferences of individuals into a community-wide (complete and transitive) ranking while also meeting a pre-specified set of [fairness] criteria.
>
> Fairness criteria:
>
> - If every voter prefers alternative X over alternative Y, then the group prefers X over Y.
> - If every voter's preference between X and Y remains unchanged, then the group's preference between X and Y will also remain unchanged (even if voters' preferences between other pairs like X and Z, Y and Z, or Z and W change).
> - There is no "dictator": no single voter possesses the power to always determine the group's preference. `https://en.wikipedia.org/wiki/Arrow%27s_impossibility_theorem`

The following example illustrates Arrow's impossibility theorem:

3.2.2.2 Condorcet's Paradox

Condorcet's paradox is a paradox which demonstrates that the collective preferences of voting actors can be cyclical (non-transitive), despite the individual preferences of the voting actor's choices being non-cyclical.

The following example illustrates Condorcet's paradox:

> Suppose we have 3 voting actors: A, B, and C voting for choices X, Y, and Z. They rank their votes sequentially from 1 to 3; lower numbers indicating a more favorable choice.

	X	**Y**	**Z**
A	1	2	3
B	2	3	1
C	3	1	2

A favors X > Y > Z. B favors Z > X > Y. C favors Y > Z > X.

It's clear from this that choice X is preferred to Y, choice Y is preferred to Z, and choice Z is preferred to X; a paradoxical result (X > Y, and Y > Z, and Z > X).

3.2.3 Practice

In practice implementing a voting system is a massive undertaking. Major elections in the US dictate how and what polices will be implemented over the next several years. As such, there are serious risks and concerns that must be considered when attempting to actually build such a system. First and foremost, an implemented voting system should protect the voting actors; second, such a system should ensure that the voting process itself is secure (resistant to corruption and manipulation); finally an implemented voting system must be scalable to be effective in large-scale elections.

Voting systems in practice require a process which enables a voting actor to cast a vote, this voting process consists of four components: registration, verification, vote casting, and collection and processing.

3.2.3.1 Voting Process

3.2.3.1.1 Registration

The **registration** component of the voting process is how the collection of eligible voters is established. The registration process varies from state to state in the US. Some states allow *election day registration*, a process whereby you can register to vote in major federal elections on the same day you vote; however,

most states require their citizens to register themselves before the election in order to have enough time to disseminate the collection of eligible voters to polling station officials. Several states require that the voting actor register up to 30 days before the day of the vote. Currently only five states in the US have automatic voter registration, or "opt-out" registration, a process by which citizens of that state are automatically granted voting rights in upcoming elections if they meet eligible voter requirements, e.g., are over the age of 18.

3.2.3.1.2 Verification, Authentication, and Authorization

The **verification** component of a vote is the process by which a voting actor provides some form of identification in order prove they are who they claim to be. The identity is then **authenticated** via some data source by a polling station. After the polling station has confirmed that the voting actor is who they claim to be and is also registered to vote, the polling place will **authorize** the voting actor to cast their vote. These steps combined with the registration process prevent what is known as **Sybil attacks** in peer-to-peer networks, an attack on a system by creating false identities to gain influence over a system.

3.2.3.1.3 Vote Casting

The next step in the voting process is **vote casting**, the voting actor is given a ballot and a place submit their choice(s). The US doesn't have a consistent vote casting process across states; some states use paper ballots, others use mechanical voting machines, and others use electronic machines. Special precautions must be taken here to ensure that votes are cast securely and privately.

3.2.3.1.4 Collection and Processing

The final step of the voting process is the **collection and processing** component. This step requires that the polling places aggregate and tally all of the votes to determine a final result. Records must be kept which would provide a means to audit and recount votes if necessary. In electronic machines the col-

lection and tallying process would be done by reading *. Mechanical machines *. Paper ballots, perhaps the most difficult, require *.

3.2.3.2 System

3.2.3.2.1 Ballot

As it turns out the ballot and the vote casting process are very dependent on one another. How the ballot is cast is an important part of protecting the voter and securing the voting system itself.

3.2.3.2.1.1 Secret Ballot

A **secret ballot** is a ballot which anonymizes a voting actor's choice. This is done for several reasons, namely to prevent voter intimidation and vote buying. Secret ballots are a right provided by several treaties; e.g., the *Universal Declaration of Human Rights*, the *American Convention on Human Rights*, and the *Convention on the Standards of Democratic Elections, Electoral Rights and Freedoms*. Secret ballots are one of the most important rights offered by democratic societies, it allows voters to vote on topics without fear of retaliation or outcast by the rest of society. However, the term secret *ballot* is somewhat of a misnomer; a secret ballot is generally a normal ballot that is cast in such a way that it wouldn't be possible to know who cast the ballot. Imagine, for example, if everyone's paper ballots were dropped into a sealed box while no one was watching.

Voting booths are used ubiquitously across the world. A voting booth is typically considered to be a small room with curtains in place to protect a voter's privacy.

While there are many benefits to secret ballots, secret ballots are not always necessary or good to have during a voting process. For example, if a unanimous vote were required on a topic it might be helpful for individuals to make their opinions public to promote discussion. Another example would be if a representative were voting on a citizen's behalf, for the sake of transparency, an open

ballot would be more appropriate.

3.2.3.2.1.2 Electronic Machines

These universal democratic principles can be summarized as a list of fundamental requirements, or 'six commandments', for electronic voting systems[citation needed]:

1. Keep each voter's choice an inviolable secret.
2. Allow each eligible voter to vote only once, and only for those offices for which he/she is authorized to cast a vote.
3. Do not permit tampering with the voting systems operations, nor allow voters to sell their votes.
4. Report all votes accurately
5. The voting system shall remain operable throughout each election.
6. Keep an audit trail to detect any breach of [2] and [4] but without violating [1].

3.2.3.2.2 Tallying Method

3.2.3.2.2.1 Voting

There are four important components of any voting system: registration, authentication, vote casting, and vote counting.

3.2.3.2.2.1.1 Vote Casting

Privacy implemented via **secret ballot**.

3.2.3.3 Risks

There are a number of risks involved with an actual election:

Election fraud:

- machine rigging,
- bribing officials,
- etc.

Voter fraud:

- vote buying,
- ballot stuffing,
- intimidation,
- etc.

3.3 Blockchain Technology

A blockchain is a distributed transactional database system that tracks transactions in ever-growing linked blocks. Blockchain technology has been used to create immutable (?) public ledgers for tracking currency, assets, and rights data. The most notable technology leveraging blockchain technology today is Bitcoin.

Blockchain technology exists to provide a solution to the Byzantine Generals' Problem in a distributed computing environment. It allows parties on an untrusted and unreliable network to build a trusted source of truth. A blockchain uses an algorithm to score different versions of history to reach consensus in the network.

3.3.1 Bitcoin

In 2008 the seminal white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, was published under the moniker Satoshi Nakamoto. This white paper outlined ideas for a new form of currency, Bitcoin. Bitcoin promised to be the first of its kind; in theory it would be the world's first decentralized digital currency which would require no trust to authenticate timestamped transactions.

It would do this by combining cryptography, a proof-of-work system, and "miners" to create a revolutionary new concept which is now known as blockchain technology. In short, blockchain technology enables enables individuals who do not trust one another to reach consensus via a trustless platform.

3.3.1.1 Network

The Bitcoin network is structured as a peer-to-peer network with a variety of nodes and node functionalities.

3.3.1.1.1 Functionality

Nodes in the bitcoin network have various functionality depending on their use case:

- A **miner** creates new blocks by solving proof-of-work problems.
- A **wallet** offers users a way to manage their keys plus send and receive transactions.
- A copy of the **full blockchain** allows nodes to verify transactions independent of other nodes in the network.
- Node **network routing** functionality allows nodes to propagate transactions and discover new nodes.

3.3.1.1.2 Node Types

There are various types of nodes on the bitcoin network. They are classified by their functionalities

- A **reference client** contains wallet, miner, a full copy of the blockchain, and network routing functionality.
- A **full node** contains a fully copy of the blockchain and network routing functionality.

- A **mining node** contains a miner, a full copy of the blockchain, and network routing functionality.
- A **lightweight wallet** contains a wallet and network routing functionality. These nodes depend on *full nodes* to verify transactions for them. These nodes are usually found on mobile device where storage is limited and the size of the blockchain is inhibitive.

The variety of nodes within the bitcoin ecosystem actually extends beyond this to include things such as pool miners and various other protocols to optimize the network for various use cases (ignored for the sake of brevity).

3.3.1.2 The Blockchain

The bitcoin blockchain is a linked list of blocks. Each block contains a set of transactions and a reference to the previous block in the chain. The block is identified by a SHA-256 hash of its header. It's helpful to imagine the blockchain as being blocks stacked vertically, each additional block helping to secure the previous blocks.

Blockchain Stack

Block #
Block 9
Block 8
...
Block 1
Block 0

Block Structure

Size	**Field**	**Description**
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Source: Mastering Bitcoin

Block Header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the Merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the proof-of-work algorithm

Source: Mastering Bitcoin

3.3.1.2.1 Merkle Trees

A Merkle tree is a data structure that allows one to efficiently verify the contents of a large amount of data. Merkle trees are used extensively in peer-to-peer networks to ensure that blocks of data arrive unaltered and undamaged. The root of a Merkle tree is called a Merkle root. Merkle trees are composed of nodes of hashes. They have the unique property of allowing the verification of the existence of a hash in the tree in log(N) time.

3.3.1.2.2 Proof-of-Work

The bitcoin protocol uses a **Proof-Of-Work (POW)** algorithm, similar to hashcash, that Satoshi Nakamoto proposed. The goal of the proof-of-work algorithm is to create a problem that is easy to verify for correctness but difficult to solve for (read: NP-complete (?)).

The proof-of-work algorithm provides a means for mining nodes to be pseudorandomly selected to build a block of transactions. The probability that a miner will be selected is directly tied to the amount of *work* a miner does.

3.3.1.2.2.1 Algorithm

The proof-of-work algorithm depends on the SHA-256 algorithm. **SHA-256**, a member of the **Secure Hash Algorithm 2 (SHA-2)** family, is a cryptographic hash function that produces a 256-bit, 32-byte, hash result.

The main properties of a **cryptographic hash function** are that it be:

- deterministic, i.e., the same input will always produce the same output,
- quick to compute,
- infeasible to determine the input from the output, i.e., a small change in the input will produce a major, seemingly random, change to the output, and
- infeasible to find a collision in resulting hashes.

These properties of cryptographic hash functions provide **collision resistance** meaning it is computationally impossible to find an input that produces a randomly selected hash output. This property can be used as a sort of pseudorandom selection.

3.3.1.2.2.2 Difficulty

The Bitcoin network has a global **difficulty** — a 256-bit value, 32-bytes — that is recalculated every 2016 blocks. The value is recalculated such that the pseudorandom selection process takes approximately 10 minutes to complete for each block.

In actuality, miners aren't "selected" to build a block, so much as have a chance of building a correct block at a probability of `(miner_hashrate/network_hashrate)`.

By using the hash of the previous block in the blockchain combined with a **nonce**, a value the miner selects, they have a chance of finding a nonce such that when combined with the previous block's hash (and current block's data) is less than the current difficulty. This is considered a correct solution and the "work" required in Proof-of-Work.

3.3.1.2.2.3 Network

If a miner finds a solution it will propagate its solution into the network. Once other nodes have verified that the solution is correct they will accept that block as correct, append it to their chain, and reward the miner with a coinbase reward, a sum of bitcoin.

3.3.1.2.2.4 Security

These properties, combined with the incentive of coinbase rewards, provide security in the form of cryptography, electricity, and hardware. Attacks that would threaten this security depend on breaking the cryptographic primitives in action, finding ways of reducing electricity/hardware costs to out perform the rest of the network in the PoW algorithm, attacking nodes in the network, or colluding with other nodes in the network to out perform the remainder of the network.

3.3.2 Ethereum

Since 2008 there have been many advancements in the field of blockchain technology; one project advancing the field is known as Ethereum. In late 2013 a young Vitalik Buterin published a white paper: *A Next-Generation Smart Contract and Decentralized Application Platform.* This white paper expanded on many of the ideas originally presented by Satoshi Nakamoto; thus, establishing Ethereum, what many describe as "Bitcoin 2.0". Ethereum offers a medium for developers to create and publish Turing-complete smart contracts, applications, and organizations that run on top of a decentralized platform. This medium is provided via blockchain technology.

A smart contract, the digital equivalent of a legal contract, serves to form an enforceable agreement between parties. A legal contract offers enforceability through legal infrastructure: state, law, judge, magistrate, constable, etc. In contrast, Ethereum's digital counterpart, smart contracts, offer enforceability

through software; namely, a distributed ledger, transactions, and pre-written logic to replace legalese. These two systems vary in interesting ways: transparency, clarity, provability, flexibility, control, efficiency, etc.

Ethereum lays the foundation for developers to create decentralized communities and organizations. Generally speaking, an organization is a collection of people operating under a set of protocols to achieve some common goal. A decentralized organization maintains these characteristics, but the protocols under which the organization operates are defined as code as opposed to parliamentary procedure. The distinction between a decentralized community and organization is cumbersome. For the sake of understandably, they can be considered equivalent in meaning.

Chapter 4

Literature Review

> **democracy** *deÂůmocÂůraÂůcy* | *noun* A system of government in which power is vested in the people.

Democracy is a fundamental birthright for Americans, a cherished blessing which serves as the foundation for our freedom. Each generation must nourish and foster the processes of their democracy so that future generations may too reap the benefits it provides. Key to democracy is the right to vote. By voting the citizens of a democratic society can express their will to their governing body. The goal of any voting system should be that the outcome fairly represents the will of the people.

For thousands of years societies have practiced democracy, held elections, and casted votes. Technology, and its applications within voting systems, has developed markedly since then. Today the Internet pervades our lives in the form of websites, applications, peripherals and more — used for social media, banking, e-commerce, and everything in-between — this leads one wonder why it is that we haven't seen more progress in the form of Internet-based voting. Constituents, election officials, businesses, counties, states, even entire countries have requested and experimented with such systems. Internet security is robust enough to support a $100 billion industry, e-commerce, which suggests that an Internet-based voting system is at least plausible.

We've seen contentious election results both locally and abroad, as well as issues that cast doubt and concern on the validity of our democratic processes: voter suppression, gerrymandering, intimidation, ballot stuffing, destruction of audit material, etc. Internet based voting systems might help to alleviate some of these concerns. Research on end-to-end verifiable voting has seen much progress in the past few years. However, Internet voting brings with it an entirely new set of security risks and concerns that must also be addressed.

The legitimacy of a government depends on public perception. Thus, election security is a matter of national security. Voters must be certain that their votes have not unfairly manipulated or tallied to modify election results, they must feel that universal suffrage is being upheld, that all those who are eligible to vote have had the opportunity to do so, that each voter has had precisely one vote, that each vote is of equal weight, and that the privacy of each voter has been maintained.

Voting is the means through which we express ourselves. If voters lose faith in their election system they will lose faith in their election results, their elected leaders, and their democracy. Trustworthy democracy is an ambitious and worthy goal that every government should strive to realize.

4.1 Elections

Should this section actually be "remote voting"?

There have been many attempts to bring online voting to the masses. We define Internet voting as any form of voting where a marked ballot is transfered over a network, this includes transfer via fax, email, or web application (fax being included because of the widespread proliferation and usage of Internet-based fax machines).

What follows is a review of Internet-based voting systems and the policies concerning them.

4.1.1 American Elections

American elections are a massive and complicated undertaking filled with federal, state, and local legislation.

31 states in America support Internet-based voting in one form or another.

25 of these states

4.1.1.1 Overseas Voting and Remote Voting

> According to estimates from the United States Elections Project, there were 5,127,418 UOCAVA eligible voters for the 2012 U.S. general election and 5,345,814 for the 2014 U.S. general election.

4.1.1.1.1 Uniformed and Overseas Citizens Absentee Voting Act

The **Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)** was passed in 1986 to render services to merchant marines, uniformed services, and other overseas civilians. Specifically, UOCAVA mandates that overseas and military voters be able to remotely register and vote in federal elections.

4.1.1.1.2 National Voter Registration Act

The **National Voter Registration Act (NVRA)**, also known the **Motor Votor Act**, was federal law passed in 1993 that came into effect in 1995. The NRVA's goal was to increase voter registration, enhance voter participation, protect election security, and ensure states maintain accurate voter rolls. This was done by combining voter registration with obtaining a driver's license.

> The NVRA effectively forced every state to offer voter registration in combination with the single civic act performed almost universally by American adults — obtaining a driverâĂŹs license.

4.1.1.1.3 Help America Vote Act

The **Help America Vote Act (HAVA)**, passed in 2002, was legislation passed to lower barriers disabled people encountered while attempting to vote. HAVA also aimed to improve vote auditing after a large number of ballots in the 2000 election were rejected. HAVA recommended that all election systems use **Verifiable Voter Paper Audit Trail (VVPAT)** and worked to create statewide voter registration lists and identification requirements.

HAVA was also responsible for the formation of the United States **Election Assistance Commission (EAC)**. The EAC is responsible for testing, certifying, and decertifying voting equipment; developing voting machine standards; and administering funds to states so that they become HAVA compliant.

The EAC requested that the **National Institute of Standards and Technology (NIST)** create a **Voluntary Voting System Guidelines (VVSG)**.

> The purpose of the Voluntary Voting System Guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility and security capabilities required to ensure the integrity of voting systems. The VVSG specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems

4.1.1.1.4 Military and Overseas Voter Empowerment Act

The **Military and Overseas Voter Empowerment Act (MOVE)**, passed in 2009, amended UOCAVA and other statues to provide further protections to eligible citizens. Specifically the act aimed to reduce the number of ballots that are not counted due to late receipt. MOVE accomplishes this by requiring that states send absentee ballots no later that 45 days prior to election day. MOVE goes further by requiring that all registration material and blank ballots be available electronically as well as removes requirements regarding notarization

on voting applications and ballots.

4.1.2 Foreign Elections

4.1.3 American Elections

American elections are a massive and complicated undertaking filled with federal, state, and local legislation.

4.1.3.1 Legislation

Interestingly, neither the Bill of Rights nor the US Constitution originally spelled out any right to vote, active suffrage, for the citizens of its democracy. It wasn't until the Fifteenth Amendment was ratified that the right to vote for citizens and the protections for citizen's right to vote were finally recognized at a federal level. In total we've had four separate amendments to the Constitution which concern voting rights:

- **Fifteenth Amendment** - Racial suffrage (1870)

  > The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any state on account of race, color, or previous condition of servitude.

- **Nineteenth Amendment** - Sexual suffrage (1920)

  > The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any on account of sex.

- **Twenty-fourth Amendment** - Financial suffrage (1964)

  > The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States

or any State by reason of failure to pay any poll tax or other tax.

- **Twenty-sixth Amendment** - Age suffrage (1971)

  The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any State by reason of failure to pay any poll tax or other tax.

The United States still does not offer universal suffrage to its citizens, e.g., felons are disenfranchised.

There are several major pieces of legislation relevant to voting rights. Many of these statutes provide basic voting rights and others go further to ensure that these rights are upheld for various demographics via varied enforcement policies.

4.1.3.1.1 Voting Rights Act

Although the Fifteenth Amendment of the Constitution was ratified in 1870 it wasn't until the **Voting Rights Act (VRA)**, passed in 1965, that the Fifteenth Amendment was actually enforced. The act laid out a number of provisions used to regulate election administration. Prior to the VRA southern states would disenfranchise racial minorities via Jim Crow laws, election fraud, voter restrictions: literacy tests, poll taxes, property-ownership requirements, moral character tests, requirements that voter registration applicants interpret particular documents, etc.

4.1.3.1.2 Uniformed and Overseas Citizens Absentee Voting Act

The **Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)** was passed in 1986 to render services to merchant marines, uniformed services, and other overseas civilians. Specifically, UOCAVA mandates that

overseas and military voters be able to remotely register and vote in federal elections. The **Federal Voting Assistance Program (FVAP)**, established under the **Department of Defense (DOD)**, provides voter assistance, tools, and education to overseas voters so that they are able to vote from anywhere in the world.

4.1.3.1.3 National Voter Registration Act

The **National Voter Registration Act (NVRA)**, also known the **Motor Votor Act**, was federal law passed in 1993 that came into effect in 1995. The NRVA's goal was to increase voter registration, enhance voter participation, protect election security, and ensure states maintain accurate voter rolls. This was done by combining voter registration with obtaining a driver's license.

> The NVRA effectively forced every state to offer voter registration in combination with the single civic act performed almost universally by American adults — obtaining a driverâĂŹs license.

4.1.3.1.4 Help America Vote Act

The **Help America Vote Act (HAVA)**, passed in 2002, was legislation passed to lower barriers disabled people encountered while attempting to vote. HAVA also aimed to improve vote auditing after a large number of ballots in the 2000 election were rejected. HAVA recommended that all election systems use **Verifiable Voter Paper Audit Trail (VVPAT)** and worked to create statewide voter registration lists and identification requirements.

HAVA was also responsible for the formation of the United States **Election Assistance Commission (EAC)**. The EAC is responsible for testing, certifying, and decertifying voting equipment; developing voting machine standards; and administering funds to states so that they become HAVA compliant.

The EAC requested that the **National Institute of Standards and Technology (NIST)** create a **Voluntary Voting System Guidelines (VVSG)**

which cover equipment, documentation, and testing requirements of voting machines.

> The purpose of the Voluntary Voting System Guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility and security capabilities required to ensure the integrity of voting systems. The VVSG specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems

HAVA also established provisional ballots for states that don't allow same-day registration. Provisional ballots allow voters to cast a ballot on election day if the voter feels they're entitled to vote but are not listed as being registered. The ballot is counted after the voter's eligibility has been verified with the goal being that no voter is turned away who should have otherwise been able to vote.

4.1.3.1.5 Military and Overseas Voter Empowerment Act

The **Military and Overseas Voter Empowerment Act (MOVE)**, passed in 2009, amended UOCAVA and other statues to provide further protections to eligible citizens. Specifically the act aimed to reduce the number of ballots that are not counted due to late receipt. MOVE accomplishes this by requiring that states send absentee ballots no later that 45 days prior to election day. MOVE goes further by requiring that all registration material and blank ballots be available electronically as well as removes requirements regarding notarization on voting applications and ballots.

4.1.3.1.6 Voter Empowerment Act

2013

4.1.3.2 Voting

Voting procedure varies depending on state legislation. Here we review early voting, remote voting, and Internet voting by state. Remote voting is a form of early voting and Internet voting a form of remote voting.

4.1.3.2.1 Early Voting

Early voting is a service that allows voters to cast ballots before election day during a specified time frame at a polling location. Some states offer early voting through **in-person absentee voting**: a voter receives a ballot through mail or internet, marks said ballot, then casts their vote at an official polling location before Election Day.

Early voting has become a popular means of voting for American citizens. In the 1980s fewer that 5% of ballots cast in the general election were cast before election day, by 2000 16% percent of votes for president were cast early, and by 2012 the number of votes casted early had risen to at least 31%.

4.1.3.2.1.1 Arguments

Proponents of early voting would argue that early voting makes the voting process more convenient for citizens, thus increasing voter turnout. Voters would have more flexibility to work around children, jobs, doctor's appointments, out of state trips, as well as be able to avoid long lines on election day.

Critics argue that those concerns are less important when compared to the risks it presents.

> Citizens should vote with a common base of information about candidates. If they vote over a period of weeks before Election Day, they vote based on the knowledge available on a scattering of different dates.

4.1.3.2.1.2 State Breakdown

34 states and the District of Columbia allow any qualified voter to vote early without excuse or justification:

1. Alaska
2. Arizona
3. Arkansas
4. California
5. D.C.
6. Florida
7. Georgia
8. Hawaii
9. Idaho
10. Illinois
11. Indiana
12. Iowa
13. Kansas
14. Louisiana
15. Maine
16. Maryland
17. Massachusetts
18. Minnesota
19. Montana

20. Nebraska
21. Nevada
22. New Jersey
23. New Mexico
24. North Carolina
25. North Dakota
26. Ohio
27. Oklahoma
28. South Dakota
29. Tennessee
30. Texas
31. Utah
32. Vermont
33. West Virginia
34. Wisconsin
35. Wyoming

3 states are remote/early voting exclusively (by mail):

1. Colorado
2. Oregon
3. Washington

4.1.3.2.2 Remote Voting

Remote voting, in contrast to early voting, is any form of voting where ballots are not marked and cast at an official polling place. Remote voting is also known as **absentee voting**. The medium through which a marked absentee ballot is returned to election officials depends on the state.

4.1.3.2.2.1 Arguments

Remote voting offers flexibility above and beyond early voting. Remote voting allows voters to vote from the comfort of their own homes, overseas, and even from space. However, there are risks associated with remote voting: voter intimidation, vote buying, vote manipulation, etc.

> Growing use of absentee voting has turned this area of voting into the most likely opportunity for election fraud now encountered by law enforcement officials. These cases are especially difficult to prosecute, since the misuse of a voterâĂŹs ballot or the pressure on voters occurs away from the polling place or any other outside scrutiny. These opportunities for abuse should be contained, not enlarged.

4.1.3.2.2.2 State Breakdown

27 states and the District of Columbia permit any qualified voter to vote absentee, without offering an excuse, via postal service:

1. Alaska
2. Arizona
3. California
4. D.C.
5. Florida
6. Georgia

7. Hawaii
8. Idaho
9. Illinois
10. Iowa
11. Kansas
12. Maine
13. Maryland
14. Minnesota
15. Montana
16. Nebraska
17. Nevada
18. New Jersey
19. New Mexico
20. North Carolina
21. North Dakota
22. Ohio
23. Oklahoma
24. South Dakota
25. Utah
26. Vermont
27. Wisconsin
28. Wyoming

20 states require an excuse to remote vote:

1. Alabama
2. Arkansas
3. Connecticut
4. Delaware
5. Indiana
6. Kentucky
7. Louisiana
8. Massachusetts
9. Michigan
10. Mississippi
11. Missouri
12. New Hampshire
13. New York
14. Pennsylvania
15. Rhode Island
16. South Carolina
17. Tennessee
18. Texas
19. Virginia
20. West Virginia

3 states are remote/early voting exclusively (by mail):

1. Colorado

2. Oregon

3. Washington

4.1.3.2.3 Electronic Voting

Electronic voting (e-voting) is the use of electronic systems to cast and/or count votes. Electronic voting can be split into two main categories **Direct Recording Electronic (DRE)** voting machines and **optical scan voting systems**. A DRE machine records votes electronically in memory. An optical scan voting system reads ballots using scanning technology, much like Scantrons in the academic world.

4.1.3.2.3.1 Arguments

The promise of electronic voting is that it would be a faster, more transparent, secure, and accurate form of voting. Other benefits would include greater ballot language support, increased support and independence for handicapped people, less printing costs, and the ability to entirely prevent spoiled ballots.

Unfortunately the promises of electronic voting have fallen short several times. Security researchers have repeatedly demonstrated methods of attacking various e-voting machines to manipulate votes casted or the tallying process itself. As a result most states no longer offer e-voting without a **Verifiable Voter Paper Audit Trail (VVPAT)**.

Proponents and vendors of electronic voting would claim that their systems are rigorously tested, but security experts argue otherwise.

> Election law in most states requires that all voting systemsâĂŤwhether electronic or notâĂŤbe qualified by an authorized federally licensed laboratory known as an Independent Testing Authority (ITA), and then submitted to the state for certification. The ostensible purpose of these procedures it to make sure that the voting system meets

the voluntary federal voting system standards promulgated by the FEC (and in the future, by NIST), and that they conform to the stateâĂŹs election laws. It is tempting to place a lot of faith in certification procedures as a means for preventing security failures. We believe such faith is unwarranted. We argue that even a lengthy, conscientious testing and examination program by the most qualified people cannot give us the necessary security guarantees. In fact, in general, no process can, since in most cases the problem of establishing that a program meets any particular security requirement is known to be fundamentally unsolvable.

There are fundamental limits to what testing can accomplish; it is a truism of the software world that while testing can be used to verify that bugs and security vulnerabilities are present, it can never prove that they are absent.

Contrary to many peopleâĂŹs intuition, it is unlikely in the extreme that anyone, whether on the development team or not, would detect malicious logic that was deliberately disguised by a clever programmer, no matter how much effort was put into the search. It is much easier to hide a needle in a haystack than to find it.

4.1.3.2.3.2 Demonstrated Attacks

4.1.3.2.3.2.1 Diebold AccuVote-TS

4.1.3.2.3.2.2 AVS WINVote

4.1.3.2.4 Internet Voting

We define **Internet voting** as any form of voting where a marked ballot is transfered over a network, this includes transfer via fax, email, or web application (fax being included because of the widespread proliferation and usage of Internet-based fax machines).

There have been many attempts to bring about online voting in the US and abroad. Over $100 million in federal funding and decades of research and development has been spent on internet voting systems.

> In 2000 there were several other experiments with Internet voting in U.S. public elections. In some cases the votes counted officially; in others they did not. The largest and most well-known was the Arizona Democratic presidential primary, conducted by election.com (whose assets were acquired in 2003 by Accenture) in March of that year, in which approximately 85,000 votes were cast and counted. The Reform Party national primary was also conducted over the Internet that summer, as were various nonbinding Internet voting experiments in some counties of Washington, California, Arizona and elsewhere.

4.1.3.2.4.1 Arguments

Internet voting would provide all of the benefits of early, remote, and electronic voting while also inheriting all of their risks and some. The major additional risk is that Internet voting exposes the entire system to remote attack from anywhere in the world and the possibility for large-scale attacks.

The conclusion of research initiatives and academic research is that Internet voting is fundamentally impossible to accomplish while maintaining voter privacy, audit trails, and preventing large scale attacks.

> it is currently not possible to ensure the security, privacy, auditability and integrity of ballots cast over the Internet.
>
> ...
>
> federal researchers determined that secure online voting is not currently feasible
>
> ...

> The conclusive evidence that online voting cannot yet be done securely led the federal government to abandon its effort to develop a secure online voting system for the military in 2014.
>
> It is reasonable to assume that the shortcomings of ITAs with respect to DREs will carry over to their certification of Internet voting.

"A comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens" made the following arguments against voting systems:

- Paperless (non-VVPAT) voting systems have been widely criticized: closed source software, insufficient scruity, insider attack potential, and no VVPAT.
- Cyber attack potential: insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks, etc.
- Attacks could occur at a large-scale and launched by individual, corporate, or state actors that may lie outside the reach of US law. Attacks could result in widespread or selective voter disenfranchisement, vote buying/selling, vote switching, etc. These attacks are capable of being perpetrated without detection.
- These vulnerabilities cannot be eliminated without a wholesale redesign and replacement of both the internet and PC.
- Seemingly successful Internet voting systems may appear to work flawlessly, promoting expansion of an insecure system.
- Not detecting a successful attack does not mean that one has not occurred.
- Because the threat of large-scale cyber attacks is so great, "we recommend against any Internet voting until both the Internet and the world's home computer infrastructure have been fundamentally redesigned."

4.1.3.2.4.2 Demonstrated Attacks

4.1.3.2.4.2.1 Voting Over the Internet

The **Voting Over the Interet (VOI)** system

4.1.3.2.4.2.2 Secure Electronic Registration and Voting Experiment

The **Secure Electronic Registration and Voting Experiment (SERVE)** was an internet voting system built under the DOD's FVAP to be deployed for the 2004 elections. The goal was to produce a voting system that reduced barriers for American voters living overseas.

4.1.3.2.4.2.3 IVAS

4.1.3.2.4.2.4 D.C. Voting System

Typically early voting

20 states have

31 states in America support Internet-based voting in one form or another.

25 of these states

4.1.3.2.5 Tables

State	**In-Person**	**By Mail**		
	Early Voting	No-Excuse Absentee	Absentee; Excuse Required	All-Mail Voting
———————-	———————-	————————	————————————	————————
Alabama			*	
Alaska	*	*		(1)
Arizona	*	*		(1)
Arkansas	*		*	(1)
California	*	*		(1)
Colorado				*
Connecticut			*	
Delaware			*	
D.C.	*	*		
Florida	*	*		(1)
Georgia	*	*		
Hawaii	*	*		(1)
Idaho	(2)	*		(1)
Illinois	*	*		
Indiana	(2)		*	
Iowa	(2)	*		
Kansas	*	*		(1)
Kentucky			*	
Louisiana	*		*	
Maine	(2)	*		
Maryland	*	*		(1)
Massachusetts	(3)		*	
Michigan			*	
Minnesota	(2)	*		(1)
Mississippi			*	
Missouri			*	(1)
Montana	(2)	*		(1)
Nebraska	*	*		(1)
Nevada	*	*		(1)
New Hampshire			*	
New Jersey	(2)	*		(1)
New Mexico	*	*		(1)
New York			*	
North Carolina	*	*		
North Dakota	*	*		(1)
Ohio	(2)	*		

Source: National Conference of State Legislatures, January 2016.

1. Certain elections may be held entirely by mail. The circumstances under which all-mail elections are permitted vary from state to state.

2. Although these states do not have Early Voting in the traditional sense, within a certain period of time before an election they do allow a voter to apply in person for an absentee ballot (without an excuse) and cast that ballot in one trip to an election officialâĂŹs office. This is often known as "in-person absentee" voting.

3. Massachusetts has Early Voting only during even-year November elections, beginning in 2016. Currently it does not permit Early Voting in primaries or municipal elections.

4.1.4 Foreign Elections

There are foreign elections worth reviewing for their voting processes and systems.

4.1.4.1 Estonia

Estonia began using Internet voting in 2005. By the 2015 Estonian parliamentary elections 30.5% of all voters voted over the Internet. Estonia maintains what are probably the most advanced national identification cards in the world. Estonian IDs are part of a **Public Key Infrastructure (PKI)** where IDs serve as smart cards which possess two RSA key pairs: one for signing and one for authentication. Cryptographic functions are performed on the card. The signatures produced by the IDs are used extensively throughout the country and are legally binding. These cryptographic IDs allow Estonia to provide voter authentication capabilities that cannot be reproduced in the US. Despite the advanced authentication capabilities that Estonia offers researchers in 2014 devised a number of attacks that could be performed on the Estonian voting system

to spoil ballots, damage ballot secrecy, and steal/drop votes. The researchers also criticized the transparency and operational security of the system.

4.1.5 Contentious Elections

Despite having had thousands of years to improve on our election systems we continue to see contentious election results both locally and abroad. What follows are some of the more egregious and contentious election results.

4.1.5.1 American Elections

4.1.5.1.1 Bush vs Gore (2000 - United States)

4.1.5.1.2 Trump vs Clinton (2016 - United States)

> "A 58 percent majority of Clinton supporters say they accept TrumpâĂŹs election, while 33 percent do not. Questions about TrumpâĂŹs victory are passionate âĂŤ 27 percent of Clinton supporters feel âĂIJstronglyâĂİ he did not win legitimately."

4.1.5.2 Foreign Elections

4.1.5.2.1 Gortari vs CÃąrdenas (1988 - Mexico)

4.1.6 End-to-End Verifiability

An **End-to-End Verifiabile (E2E-V)** voting system is a system that provides the following features for voters:

- allows voters to check that the system recorded their votes correctly,
- allows voters to check that the system included their votes in the final tally, and
- allows voters to count the recorded votes and double-check the announced outcome of the election.

E2E-V voting systems have been a hotbed of research over the past several years. An **End-to-End Verifiable Internet Voting (E2E-VIV)** is an E2E-V voting system that allows you to vote over the Internet.

> "Aggressive early adoption of election technology must be tempered by a clear understanding that votersâĂŹ trust in their elections is hard-won and easily lost."

4.1.6.1 Technical Requirements

A 2015 study on, End-to-End Verifiable Internet Voting determined ten technical requirements of E2E-VIV systems:

- functional
- accessibility
- usability
- security
- authentication
- auditing
- system operational
- reliability
- interoperability
- certification

4.1.6.1.1 Functional

> The functional requirements of an E2E-VIV system deal primarily with the casting and recording of ballots and associated voter records.

Receipt freedom is one such functional requirement, a property where it is impossible for a voter to prove to anybody how they voted.

Others include:

- Ensuring that a voter cast a ballot if such an act is recorded.
- Data retention in case of failure.
- Multi-vote functionality to overwrite a previous votes.
- Maintaining voter anonymity.

4.1.6.1.2 Usability

> The usability of an E2E-VIV system is critical to its successful adoption and use.

Usability is mostly concerned with user experience and confirmation guarantees. For example, voters should be confident that their vote was cast by being provided a confirmation screen. The voting process should be both intuitive and guide the voter through the process. Presentations such as the butterfly ballot should be avoided at all costs.

4.1.6.1.3 Accessibility

> **Accessibility** is the property of being usable by and useful to voters with disabilities.

Digital voting systems have the potential to provide wider accessibility guarantees than traditional paper ballots. To provide these guarantees developers must involve voters throughout the development process to identify accessibility issues and implement solutions.

4.1.6.1.4 Security

Security is one of the most integral properties to maintain for voting systems. Included in this requirement is that:

- No data can be permanently lost.
- Integrity of voters, candidates, ballot information, cast ballots, and other critical information must be maintained.
- Accurate timing information is critical for auditing.
- System must perform regular health checks.
- Voting equipment must be protected.
- The system must perform regular health checks.

4.1.6.1.5 Authentication

Authentication is the process of ascertaining the validity of a claimed identity. Authentication ensures that the voting system can enforce privacy and prevent multi-voting, Sybil attacks, and vote theft. All individuals must be identified uniquely.

The system must allow access to services only to authorized users, e.g., only allow election officials to load ballot info.

4.1.6.1.6 Auditing

The property of **auditability** means that a voting system is capable of comprehensive examination. Auditability must exist at all stages and levels of the voting process. The system must keep auditable logs of all relevant activity and the logs must be public and write only. Furthermore, the logs cannot leak any data regarding voters or the way any ballot was cast. Privacy must always be the foremost concern.

The auditing system must actively report issues and information in real-time. At least the following events should be recorded:

- all voting-related information, including the number of eligible voters and votes cast, the number of invalid votes, count and recount results, etc.;

- any detected attacks on the operation of the system or its communication infrastructure; and
- any system failures, malfunctions, or other detected threats to proper system operation.

And at least the following features must exist:

- cross-check and verify the correct operation of the voting system and the accuracy of the election results;
- detect voter fraud; and
- prove that all counted votes are legitimate and that all ballots have been counted.

Auditability must extend to the source code, actions performed, and documentation itself.

4.1.6.1.7 System Operational

System operational requirements are those that enforce and regulate transparency, accountability, system configuration, and updates. Logs: software used, configurations, versions, updates, etc. must all be managed and produced to audit for tampering. Protocols should be in place to guard sensitive equipment at all times and handle system failures. Officials managing these systems and the procedures themselves must be scrutinized closely to prevent insider attacks and election fraud.

4.1.6.1.8 Reliability

Reliability is the property of a system behaving reasonably and as expected under both normal conditions and while under attack.

During an election period a system should be highly available. 99.9% availability is a minimum for voting systems. The system must also be able to recover

from any failure within 10 minutes, with the exception for failure caused by natural disaster or malicious attack. The system should have redundant backup systems for critical components of the system.

Internet voting systems are compelling targets for **Distributed Denial of Service (DDoS)** attacks, therefore it's important that an E2E-VIV system be able to continue operation with correctness during a sustained DDoS.

4.1.6.1.9 Interoperability

An E2E-VIV system must use open standards for interoperability between components, services, and other E2E-VIV systems. Logs and documentation of such standards must be published so that anybody can download, inspect, and publish analysis and concerns.

4.1.6.1.10 Certification

There should be tests involved for every functional requirement; these tests should be able to be run on demand. Formal proofs of security and correctness should be provided wherever possible. Third parties should also review, audit, and test the system.

4.1.6.2 Non-Functional Requirements

The same 2015 study study found 5 non-functional requirements for an E2E-VIV systems:

- operational
- procedural
- legal
- assurance
- maintenance/evolvability

4.1.6.2.1 Operational

Within the operational requirements the authors describe several operational requirements: voter assistance, election and registration timing, voter registration, candidate nominations and lists receipt freedom, voter assistance, election integrity, and openness.

4.1.6.2.1.1 Voter Assistance

Voters must be well informed on how to register, vote, and protect their privacy in the voting system.

4.1.6.2.1.2 Election and Registration Timing

Clear instruction on when voting and registration occurs should be announced far in advance for the voters benefits. When multiple forms of remote voting take place votes cast over the Internet should not be accepted after other forms of remote voting end.

4.1.6.2.1.3 Voter Registration

E2E-VIV systems must publish a voters' register that is regularly updated. Voters should be able to check that information in the register is accurate and request corrections.

4.1.6.2.1.4 Candidate Nominations and Lists

The ballot presented to voters must be consistent, fair, unbiased, and free from any superfluous information about candidates/choices.

4.1.6.2.1.5 Receipt Freedom

Operational receipt freedom represents two different requirements depending on whether a voter is voting from a supervised or unsupervised location.

In a supervised location receipt freedom requires that the voting terminal clear all indication of how a ballot was cast and ensure that no paper trail

representing how the ballot was cast is able to leave the polling place (except by official means).

In an unsupervised location any visual proof of vote should not be able to be used to determine how a vote was cast or will be tallied.

4.1.6.2.1.6 Election Integrity

If test ballots are able to be submitted then those ballots must be clearly marked as a test ballot with instruction on how to cast a real ballot.

The voting system should not disclose any results to any person until after the voting period has ended, including alternative forms of voting. Tallying should be done as soon as possible afterwards. The tallying process should be transparent, recorded, and be able to be replayed.

Irregularities which affect the integrity of votes should be recorded.

4.1.6.2.1.7 Openness

An E2E-VIV system must be open and function properly regardless of the hardware and software stack the voting machine is running.

4.1.6.2.2 Procedural

Procedural requirements define the processes required to deploy and run the E2E-VIV system. Procedures should be published regarding provisioning, certification, maintenance, availability, and use.

For example, when updates occur, election officials must call upon an independent body to perform verifications of performance and certification of intent.

Procedures should be in place to teach voters the voting process and election officials should have maintenance and security procedures to ensure that voting equipment is operating nominally and has not been tampered with. An example of a security procedure would be enforcing that teams of at least two people be required to perform sensitive operations.

As much as possible there should be procedures in place to allow observers to watch election procedures.

Procedures should be in place in the event that a voter proves that their vote was not accurately received or counted.

4.1.6.2.3 Legal

There are a number of national, state, and local law that apply to voting systems, e.g., accessibility, anonymity, and availability guarantees. Any deployed E2E-VIV system must comply with these laws.

Election officials must ensure that only one vote by each voter is counted. This is especially relevant when multiple means of voting exist, e.g., remote and traditional vote.

Voters must be able to restart, discard, or alter their votes at any point during a voting process. The system must allow the voter to participate in an election without marking choices, i.e., casting blank or partially blank ballots. The voting system must always preserve anonymity and indicate clearly that the voters ballot has been cast and voting procedure completed.

> There must be no impediments to interested parties who want to study the E2E-VIV system. In particular, no nondisclosure agreement or contract of any kind may be required for download and study of, or for building, testing and publishing test results for, the E2E-VIV system.

4.1.6.2.4 Assurance

Client-side software must be functional and free of bugs across a wide range of hardware and software stack combinations. There must be strong security with respect to authentication such that voter credentials cannot be forged or invalidated without breaking underlying cryptographic protocols.

The entirety of the voting system — e.g., software, documentation, design, architecture, algorithms, build scripts, issue tracking system, etc. — must be

free, open, and public. All available resources should be up to date, certified, and released under license that permits anyone to download, build, test, or modify the source.

4.1.6.2.5 Maintenance and Evolvability

Election officials must have the right and ability to update the election system to conform to law, technology, or threat independent of the original vendor (read: the software must be free).

4.1.7 Architecture

There are over 127,000 possible architectural variants. They are modeled as follows:

```
static_diagram E2EVIV_Architecture_Dimensions
    -- This diagram shows the various dimensions of an E2EVIV architecture
component
    class E2EVIV_ARCHITECTURE
    feature
        authority_distribution: SET[VALUE]
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                    it_holds v member_of { Centralized, Distributed };
            end
        crypto_protocols: SET[VALUE]
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                    it_holds v member_of { On_Paper, Mechanized,
                                           Verified, Generated };
            end
        correctness_evidence: SET[VALUE]
```

```
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                it_holds v member_of { Process_Based, Assertions };
            end
        implementation_type: SET[VALUE]
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                    it_holds v member_of { Golden_Implementation,
                                           Open_Protocols_and_Specs };
            end
        key_distribution_method: SET[VALUE]
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                    it_holds v member_of { Public_Ceremony, Threshold_Cryptography,
                                           PKI, Web_of_Trust };
            end
        deployment_style: SET[VALUE]
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                    it_holds v member_of { Trusted_Servers, Public_Cloud, Peer_to_Peer };
            end
        client_technology: SET[VALUE]
            ensure 0 < Result.count;
                for_all v: VALUE such_that v member_of Result
                    it_holds v member_of { Custom_App, Web_Based };
            end
    end
end
```

4.1.8 E2E-V Voting Systems

What follows is a review of E2E-V systems currently in existence.

4.1.8.1 Demos

4.1.8.2 Helios

4.1.8.3 Norwegian System

4.1.8.4 Remotegrity

4.1.8.5 RIES

4.1.8.6 Wombat

4.1.8.7 vVote

Chapter 5

methods

Chapter 6

results

Chapter 7

discussion

Chapter 8

conclusion