Voatz: A Secure Vote in Every Hand

Leveraging Security and Technology to Increase Voter Participation

Table of Contents

Executive Summary

Taking advantage of a recent confluence of technology advancements—the ubiquitous smartphone, remote digital identity proofing, the secure blockchain technology—and their increasing availability, Voatz has developed a secure mobile voting platform that brings polls to the palm of every voter.

A secure app available for download by eligible voters on iOS or Android smartphones, the Voatz mobile voting platform utilizes blockchain technology to record ballot submissions directly from a voter's mobile device, then securely deliver them to dedicated servers for tabulation. With the aim of providing the most secure solution at every step in the Voatz mobile voting process, the platform employs extensive security protocols before, during, and after ballot marking, including biometric authentication, third-party vetting, attack mitigation, certificate transparency, end-to-end encryption, multiple verification processes, and more. Utilizing advanced cryptography, Voatz also provides election officials with a verifiable and immutable infrastructure to protect the integrity and confidentiality of every vote.

After a highly successful pilot in the 2018 West Virginia primary election, Voatz is leveraging jurisdictional and user feedback and partnering with leading security experts to soon offer this mobile voting platform across local, state, and national elections, with the ultimate aim of enhancing voting security, eliminating voting barriers, increasing voter turnout, cutting jurisdiction costs, and providing safe, easy, and secure mobile voting from anywhere in the world.

A Confluence of Technologies, A New Voting Opportunity

In recent years, three major technology changes and advances—smartphone ubiquity, smartphone security, and the blockchain—have led to the development of a striking new opportunity for voters. Voatz, a mobile-focused election voting and citizen engagement platform, was founded on the confluence of these technologies and its potentially significant impact on the voting experience in the United States.

Smartphone Ubiquity

95% **of adults in the U.S. own a smartphone.**

-Pew Research Center

By the numbers, there are nearly three billion smartphone owners across the globe[1]. Of those, about 310 million live in the United States, where the rate of penetration surpassed 80% in 2016.[2]

Now ubiquitous, armed with biometric security capabilities, and faster and more accessible than ever, the smartphone is ideal for enhancing the voting experience without requiring new capital investment from election jurisdictions.

Smartphone Security

One key security advancement, **remote digital identity proofing**, uses the smartphone's high-resolution camera, and is now widely used to establish the validity of government-issued identification cards. Other means include "liveness" detection and facial recognition. Voatz has integrated both these technologies to ensure that voters marking a mobile ballot are both real and who they say they are.

Biometric authentication, which has become a standard feature on smartphones released after 2013 is another crucial Voatz technology, deployed at the time of ballot access to ensure voter identities are verified and linked to the correct smartphone.

Voatz adheres to the National Institute of Standards and Technology (NIST) framework when integrating third-party technologies like credential verification, consistently following best practices while staying on the cutting edge of solving identity-related security issues in U.S. elections.

Blockchain

Inherent **Blockchain** Features

Transparent: transactions are public to anyone with access to the blockchain ledger.

Verifiable: each server (node) functions to verify the authenticity of the blocks (collections of data).

Immutable: the data stored cannot be altered or destroyed.

While blockchain technology has been around for more than a decade, it began to emerge as a viable method for transferring information and data in 2016.[3]

Since then, blockchain's use has expanded far beyond just cryptocurrency—for which it is most widely recognized—into government, health care, humanitarian work, and the election process.[4]

Blockchain technology is well-vetted[5] and ideally suited for elections because it secures the aggregate vote and prevents manipulation. Blockchain's distributed ledger technology uses debits and credits similar to a general ledger, but is distributed across multiple, separated servers, not stored on a single computer.

This distributed nature allows for additional security protections against denial of service attacks, duplication of data, and single points of failure at the database or server level. The blockchain nodes leverage advanced cloud security, DNS redundancy, web application firewalls, and end-to-end encryption.

Today's Unprecedented Voting Challenges

U.S. elections to date have been plagued with a host of inefficiencies and voting obstacles. As a result, low voter turnout has been a consistent issue in U.S. elections, with only around half of registered voters casting ballots in most elections.[6] [7]

Percentage of Registered Voters Who Cast Ballots

Election Year	2008	2010	2012	2014	2018
Voter Turnout	**63%**	**41%**	**57%**	**37%**	**47%**

Mobile voting platforms like Voatz aim to increase voter participation by using voter-owned devices, and thus remove considerable friction from the election process.

Challenges to Securing Every Vote

With traditional voting channels, concerns about absentee ballot tampering or in-person voter fraud have led many jurisdictions to require government-issued photo IDs at polling stations or imposing labor-intensive signature verification processes. Other current concerns include hacking voter registration databases, malware attacks, and vulnerable voting machines.[8]

Challenges for the Overseas Military Voter

Beyond the hurdles the average voter faces when casting traditional paper ballots (notably geographic access and restrictive work schedules), registered military personnel, their spouses, dependents, and citizens stationed overseas must vote using non-secure methods such as email, fax, or postal mail. These relatively dated methods do not preserve privacy and often present burdensome inconveniences.

While almost all military members possess smartphones with internet access, voters stationed across the United States' 800 foreign military bases[9] encounter significant "infrastructure obstacles not faced by voters in the U.S.," including slow mail speed and lack of access to election news.

The participation rate for overseas voters, including deployed military who must use mail-in or email ballots, was a striking **7%** in 2012.[10] In fact, the Federal Voter Assistance Program Director, David Beirne, said in a report that, **"the voting rate of Americans living abroad would have increased from 7 percent to 37.5 percent, if overseas obstacles to voting were removed."**[11]

Mobile Voting Potential

Prevent

19,000

military and overseas **ballot rejections** due to arriving after the deadline.

Count

2.8 million

more overseas votes in each election.

Delivery Delays

Mail-in ballots frequently experience travel delays with no guarantee of delivery. Often, they arrive and are tabulated after a race has been called, leaving the overseas voter feeling disenfranchised, as if their vote doesn't really count.

Emailed and faxed ballots are transmitted via insecure methods that do not preserve voter privacy and require jurisdictions undergo a time-consuming process of recreating the paper ballot by hand, under witness of two election officials, in order to be tabulated.

Challenges to In-Person Voting

Domestic voters who make it to polling stations on Election Day are not immune to delays, conflicts, or disruptions in casting their ballots.

On general Election Day in 2018, machine malfunctions, confusion, lack of staffing, extreme weather, and locked polling stations were just a few of the obstacles that cost voters time and resources, often causing them to leave polling stations without casting ballots.[12]

Additionally, several states do not permit early voting without a pre-identified excuse or justification application, creating challenges for many with work or family obligations outside normal polling hours.

The above disruptions do not begin to tackle the perpetual voting difficulties faced by the disabled, homebound, or elderly, whose access options are further limited. Moreover, voting barriers such as extreme weather, machine malfunctions, and lack of equipment availability continue to be seen election after election.

Mobile Voting Potential[13]

Enable

73.9 million

more voting-age Americans with disabilities to mark their ballots in an environment of their choosing, utilizing their own accessible and supportive device.

High Costs and Complexity

The cost to operate a polling place is incredibly high and covers a range of expenses. Voting machines alone can range between $2,500 and $3,000, and optical paper ballot scanners can cost as much as $5,000 apiece.[14] Additional expenses include licenses, maintenance, transportation, printing, and poll worker compensation.[15] Moreover, end-of-life equipment must be replaced, or else risk vulnerable and unpatchable systems.

Mobile voting channels could start the process of replacing jurisdiction-owned voting equipment with voter-owned equipment, **reducing election costs associated with mailing out paper ballots, handling ballots, mailing in marked ballots, signature verification labor, and ballot transcription.**

Why We Need a New Mobile Voting Channel

Aware of the cost, complexity, and challenges of U.S. election voting, Voatz is addressing the most pressing needs on the minds of voters and election officials alike:

- Enhancing and ensuring voting **security**
- Offering voting **channels** that function across geography, ability, class, schedules, weather, and budgets
- Lowering the **cost** of running elections
- Improving ballot **access** and timely **tabulation** for military, overseas, and disenfranchised voters
- Improving voter **turnout** across all elections.

New Voting Possibilities

By leveraging existing technology and advanced security techniques, Voatz is using extensive election and security experience to offer **a new mobile voting channel** poised to deliver multiple benefits to voters and election officials, including heightening voting security and increasing access and turnout. By bringing the polls to voters' mobile devices—with convenience, speed, no extra expense, and without changing the jurisdiction's primary tabulation system—the Voatz channel can impact current obstacles to in-person and mail-in voting while maintaining voter privacy and stringent security standards.

Closing the Gap

Smartphone Ownership Rates[16]	vs.	Election Turnout Rates[17]
94%	18-29-year-olds	42%
89%	30-49-year-olds	58%
73%	50-64-year-olds	68%

*According to the Pew Research Center and the United States Elections Project, those with the **highest** rates of smartphone ownership have the **lowest** voter turnout rates.*

Voatz Case Study: West Virginia Mobile Voting Pilot

In the 2018 general election, the state of West Virginia piloted the Voatz platform across the state. Secretary of State Mac Warner sought to offer **"a secure military mobile voting solution that is verifiable, transparent, and more secure and accessible than currently available mobile voting systems."**[18]

Voatz Rollout Process

May 2018	Voatz conducts an election pilot across **2 West Virginia counties,** collecting votes from **7 countries.** 183 voters became eligible to vote in the pilot by checking indicating on their Federal Post Card Application form that they would like to receive their ballot online or by email.
September 2018	**Active-duty deployed military or their eligible dependents** who are West Virginia residents and registered to vote are given access to the Voatz smartphone application. **3x** as many overseas voters choose their smartphone over other methods of mobile voting. 87% of eligible overseas voters download the Voatz application from the iOS App Store or the Google Play Store. 90% of voters who downloaded the application finish the identity proofing step and automatically receive their ballot. **999 ballot styles** from 24 participating counties are formatted for a smartphone. 98% of the transmitted ballots are marked, submitted, and counted successfully. (In the 2016 General Election, only 66% of transmitted ballots were marked and submitted.) Marked mobile ballots are received from **31 countries**. The last ballot is received **10 minutes** before polls close.
November 2018	Polls close on November 5, 2018. 100% of submitted ballots undergo a post-election audit.

How Voatz Secures the Voting Infrastructure and Devices

Through every step of the mobile voting process—from making the app available for download on a voter's smartphone, to the final vote verification and tabulation—the Voatz platform employs **extensive security measures** to ensure voters can cast their ballots safely and securely in an election.

Along with the secure hiring and coding practices employed within Voatz's corporate infrastructure, additional security measures include:

Rigorous application testing

Third party vetting and verification prior to app distribution

Smartphone device security checks

Threat mitigation and avoidance techniques in ballot creation and delivery

Biometric identity validation and voter authentication

Communication and network security through ballot marking and submission

Secure vote storage on the blockchain

Anonymized yet verifiable audit trail

These and other processes ensure end-to-end safety for voters and election officials across a new mobile voting channel.

Voatz Corporate Security

The security of the Voatz platform begins with the physical, digital, and personnel security measures implemented in Voatz's corporate infrastructure.

Physical Security	Human Security
• 24-hour secure office spaces • Badge-enabled workspace access • Secure technology storage	• Extensive background checks • Strict security protocols and practices • Adherence to National Institute of Standards and Technology (NIST) frameworks

Application Security

In partnership with cybersecurity industry leaders, an extensive and rigorous testing list was developed based on industry leading frameworks, including OWASP, SANS, NIST, and MITRE. In addition to continually working to uncover top security flaws, Voatz security testing will detect flaws outside the list of common and known vulnerabilities. Third-party penetration testing will inspect the source code of the backend systems and the Voatz smartphone applications for both iOS and Android devices.

Leveraging proprietary methodologies, Voatz tests against:

- **OWASP Mobile Top 10 Risks**
- **Unintended Data Leakage**
- **Attack on Binary Protections**
- **Local and Remote Injection Attacks**
- **Information Disclosure Attacks**
- **Application Reverse Engineering or Decompilation**
- **Common Authentication and Authorization Issues**

Independent Security Vetting[19]

Public Bug Bounty Program	Federal Election Assistance Commission Testing and Certification Program
• Continuously analyzes and tests implementation of the blockchain network and mobile applications • Community vetting of upcoming platform releases • Internal infrastructure security assessments • Continuous vulnerability scans against insecure or misconfigured systems/settings	• Full accreditation of the Voatz platform's functionality, accessibility, and security • Fulfills requirement under the Help America Vote Act (HAVA) • Independent verification of compliance with national standards for integrity and reliability of voting system operation established in the Voluntary Voting System Guidelines.

Application Verification Process

Before arriving in the Apple App Store or Google Play Store, the Voatz app has been validated and automated by an EAC federally accredited voting system test lab. This third-party quality assurance process means the app arrives ready for user download with thoroughly vetted source code.

Apple verification entails conducting a detailed source code and binary analysis to search for hidden vulnerabilities, and utilizing third-party subroutines managed via CocoaPods. The code is then signed with Apple's key and the Voatz certificate, and finally test run with actual data by Apple staff, who compare against documentation and establish a usability guideline.

Google verification entails signing the app's code with their key and the Voatz certificate and conducting a full accessibility test with a detailed report.

The Voatz app is ***uploaded*** to the Apple App Store and Google Play Store and available for eligible voters to download once analyzed, vetted, and approved.

Voatz's ***trusted build*** architecture verifies upon download all dependency cryptographic signatures are exactly the same as those stored in the central repository. This verification confirms that the local cached version has not been altered and is exactly the same as the master version in the central repository.[20]

Device Security

Beyond application verification and testing, Voatz has also worked closely with Apple and Samsung to implement **several security checks within the smartphone itself**:

Latest version updates of the operating system.

Automatic app shutdown if the phone has been tampered with, i.e. being rooted or jailbroken.

Continuous detection of malware, man in the middle attacks, use of unsecured WiFi networks, or other malicious processes.

How Voatz Secures Every Ballot

The Voatz mobile voting process and its security measures begin well before an eligible voter receives their ballot.

Ballot Creation

Ballots are created based on the **election definition** (the set of files produced by the primary voting system used for rendering paper ballots and accessible devices, tabulating ballots, and assigning ballot styles to voters). **Ballot styles**, which present voters with their unique list of contests and candidate order based on geographic information) are created and delivered by:

1. Capturing election definition from the primary voting system.
2. Producing the smartphone ballots.
3. Proofing the smartphone ballot styles.
4. Sending the proper ballot style to each eligible voter.

Ballot Reformatting

Because ballots presented on a smartphone inherently look different from paper ballots, and until the primary voting system is able to automatically format ballots for smartphones' small screens, Voatz must reformat paper ballots to be accessible and mobie-friendly. Reformatting includes foreign language voter instructions, especially for ballot measures.

While reformatting ballot appearance introduces potential for error, Voatz has anticipated the threat condition.

Mitigation Event

Threat: After reformatting, the smartphone ballot is not a true representation of a voter's paper ballot style (e.g. a contest or choice was left off of the smartphone ballot).

Detection: Visual tools have been provided to the jurisdiction to manually proof the smartphone ballots against the paper ballot format produced by the certified primary voting system.

Protection: Thoroughly tested, automated tools perform the conversion and compare hashes of the election definition of the smartphone ballots to the election definition represented by the original paper ballots. Any anomalies represent a bug in the tools which must be patched.

Reformatting paper ballots to smartphone ballots also introduces potential errors in mapping precincts to voters. The following prevention technique will ensure the Voatz app delivers a correct ballot, identical to the paper ballot mapped for each voter's precinct.

Mitigation Event

Threat: Delivering the wrong ballot style to a voter, enabling them to vote for candidates or ballot measures which are not in the voter's district.

Protection: In an automated process, the voter registration system matches a voter's digital ID (see Voter Security) to its corresponding database record and provides the correct ballot style ID to be sent to the voter. Mistakes in the jurisdiction's voter file are outside the scope of the Voatz platform, however, the jurisdiction can also perform manual tests of all ballot styles and their precinct assignments using the Voatz Administrative Portal.

How Voatz Secures Your Digital Identity

Before voters are invited to download the Voatz App, each jurisdiction must perform **voter authorization** (see *Appendix B*). Once an individual's eligibility to vote has been confirmed and they have downloaded the Voatz App to their smartphone, the voter undergoes **remote identity proofing, binding, and authentication.**

The Digital Identity Process Verifies

✓ The voter's identity

✓ Jurisdiction-confirmed eligibility to vote

✓ Identity is uniquely and biometrically tied to only their smartphone

Ensuring that

✓ Only the authenticated user votes

✓ Only one vote is allowed

✓ Voting is only allowed on the authenticated device

Identity Proofing, Binding, and Authentication

Within the Voatz App on their smartphone, eligible voters will follow these steps of identity proofing, binding, and authentication in order to receive authorization to vote in an election:

Identity Proofing

Identity proofing confirms an individual is who they claim to be by matching them to a government-issued photo ID.

Voatz has partnered with a leading third-party Credential Service Provider (CSP) to integrate an extensive document recognition library into its mobile voting platform. This solution recognizes **driver's licenses**, **U.S. passports**, and **state-issued photo ID cards** from every state and U.S. territory (see *Appendix C* for the complete Identity Proofing process.)

Identity Binding

If matched, the voter's digital identity is then bound to their unique smartphone identification. The user must re-authenticate themselves in the same way they did to gain access to their phone. Binding ensures that only the identity-proofed voter can vote on the given device.

Identity Authentication

At the time of voting, authentication confirms that the individual requesting ballot access is the same individual whose identity was proofed and bound to the smartphone in use. Once authenticated, the voter is granted authorization to access and mark their blank ballot.

How Voatz Secures the Voting Process

A typical mobile ballot marking process follows the four steps below. On average, voters will navigate and mark their ballots within the Voatz App in under three minutes.

Step 1: Unlocking the Ballot

To begin the voting process, the eligible, identity-proofed voter opens and biometrically unlocks the Voatz app on their smartphone. *Failure to biometrically unlock the app will initiate additional security interventions required before the voter can proceed.* Once successfully unlocked, the voter may access their ballot to begin marking.

Step 2: Marking the Ballot

The voter's choices for candidates or other measures are made one at a time, by marking the desired choice for each contest. *Voters may not select more choices than allowed*. At any time before submission, the voter can review and adjust all choices.

Step 3: Submitting the Ballot

Once the voter submits their marked ballot, it is immediately anonymized, shuffled, and posted to the blockchain. Every ballot undergoes a secure process in order to arrive safely and anonymously to election officials for tabulation (see *Appendix D*).

Step 4: Receiving Confirmation

Throughout the ballot marking process, the Voatz App will display a "pending" message. While pending, the blockchain verifying servers are simultaneously and independently attempting to verify the ballot. Once one blockchain server performs a verification, the other servers can instantly confirm the verification.

After *every* blockchain server has confirmed the vote(s), every copy of the blockchain is updated, **a confirmation message** is sent to the voter's phone through the Voatz App. The voter also receives an **automatic, digitally-signed receipt** with their selections so they may confirm their vote was recorded properly. *If the voter attempts to vote again, the Voatz app will indicate that their vote has already been cast.*

See Appendix E for details on how votes are stored securely on the Blockchain.

Spoiling a Ballot

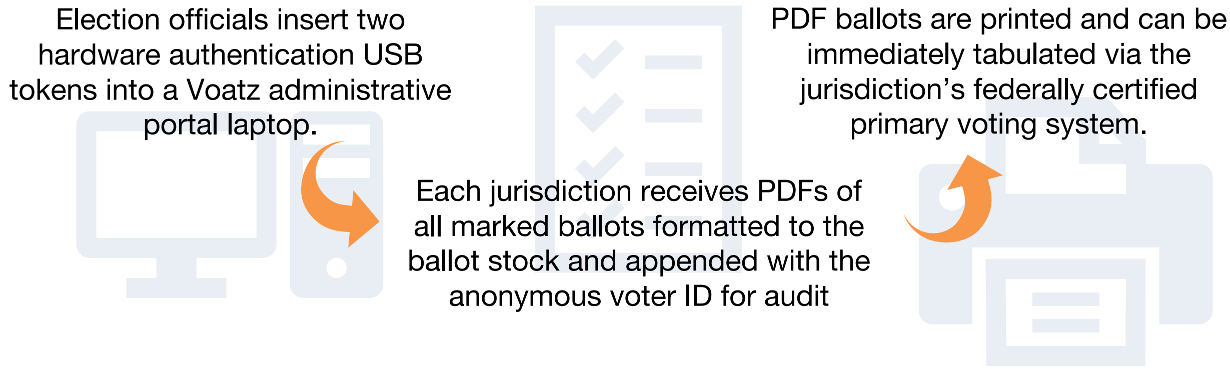
Where permitted, if a voter detects a marking error, they may *spoil their original ballot* and mark a new one. (See Appendix E)

How Voatz Ensures Post-Election Security and Review

Jurisdiction Tabulation

Once polls close, the Voatz app will no longer submit ballots. All ballots originated and marked within Voatz are stored securely on the blockchain (Appendix E), where election officials can safely access them to begin the tabulation process. **Tabulation will remain under the authority of voting jurisdictions.** Printed ballots are tallied using the standard counting process for each participating county.

How Election Officials Access Mobile Ballots



Election officials insert two hardware authentication USB tokens into a Voatz administrative portal laptop.

Each jurisdiction receives PDFs of all marked ballots formatted to the ballot stock and appended with the anonymous voter ID for audit

PDF ballots are printed and can be immediately tabulated via the jurisdiction's federally certified primary voting system.

Post-Election Audit

A voter-verified audit trail is created with printed ballots generated to match every mobile vote recorded on the blockchain. Printed ballots are tabulated anonymously but can be verified at any time.

A jurisdiction can perform audits on the mobile voting system even before ballot tabulation, by comparing:

The **number of voters** against the **number of printed ballots**

The **intended ballot style** against the **recorded ballot style**

The **number of receipts received** against the **number of ballots printed**

Conclusion

Now more than ever, voters are using handheld technology to communicate widely, exchange opinions, and engage civically. This cultural shift is measurable in the preponderance of smartphone ownership across demographics. In addition, worldwide distribution networks, infrastructure improvements, and major security advances are all converging to enhance traditional practices with remote capabilities.

At the same time, election participation issues continue to plague the democratic process for overseas military personnel and their dependents, domestic voters, elderly and disabled voters, who are all adversely challenged by the current voting channels.

Voatz aims to leverage both the technology saturation and advancements in order to increase participation across historically under-voting populations. These technological advancements stand to benefit those otherwise unable to participate and make processes such as mobile voting both a necessity and an inevitability.

Seeking to pioneer this movement, the Voatz platform introduces a new mobile voting channel, delivering ease, safety, security, and confidentiality to the voting population. Centered on security, the Voatz application utilizes blockchain technology and the most advanced security protocols to authenticate users, deliver ballots, record submissions, and provide results to election officials for tabulation.

More than 80,000 votes have been cast on the Voatz platform to date, allowing voters to civically engage where they have the highest levels of accessibility: right on their handheld devices. Contact Voatz to initiate a pilot for your area’s upcoming election.

About Voatz

Voatz is a mobile elections platform that makes it possible to vote from a mobile device by leveraging the security built into the latest versions of smartphone technology, and the immutability of the blockchain.

Voatz was co-founded in 2015 by Larry Moore and Nimit Sawhney, after winning a hackathon at SXSW with the idea that would become the early seedlings of the Voatz platform. With careers in technology, digital security and mobile payments, Moore and Sawhney combined the latest advancements in smartphone technology with biometrics and blockchain technology to make voting more accessible and secure.

Since June 2016, more than 80,000 votes have been cast on the Voatz platform across more than thirty elections. Voatz has experience working with both major political parties, churches, unions, universities, towns, cities, and states, all in the effort to make it safe, convenient and easy to vote.

Appendices: Behind the App

Appendix A: Communication and Network Security

The Voatz platform utilizes the following advanced security protocols throughout the ballot submission and confirmation process:

HTTPS and End-To-End Encryption

All communication between the user's device and the backend systems is encrypted. The Voatz platform uses TLSv1.2 (AES-GCM with RSA key agreement with SHA, SHA256, and SHA384) with additional PKI based payload encryption for the relevant API calls. Each voter's mobile device creates public and private keys during voter onboarding. At the same time, the server also creates a unique public and private key pair for each voter. The device and the server exchange public keys during the initial handshaking process, while their private keys never leave the respective systems. All data is still sent over HTTPS, but it is first encrypted by the other party's public key in such a way that only the entities holding the private keys can decrypt one another's messages.

Perfect Forward Secrecy (PFS)

While encrypted traffic is unreadable, it may still get stored on certain devices, even when caching is disabled. If a private key used to encrypt traffic is compromised, that key can be used to read all previously stored traffic. To prevent this kind of compromise, Voatz uses Perfect Forward Secrecy (PFS) to generate a one-time session key that is unique for each communication session. Thus, if the key for a specific session is compromised, it will not compromise data from any other session. The practice of PFS is used in many modern social media communication applications to reduce the risk of accidental data exposure.

Application Key Sequencing

Application Key Sequencing is used to maintain a logical sequence of events, starting with the mobile device or tablet activation, and all subsequent communications between the mobile/tablet application and the server. This detects situations in which both a rightful voter and an attacker are using the same account in parallel from different phones, or if the same voter is trying to register on more than one device. The key element here is the NEXT_KEY value, which is first generated randomly by the server upon activation and stored in the application's private data storage during the initial handshake. Upon each subsequent session establishment (login), the application sends this value to the server for validation. After this stage, the new value (for future sessions) is calculated by the server then passed to the mobile/tablet application as NEXT_KEY and the device confirms its reception. The mobile/tablet application will use this value the next time it needs to establish the session. Note that Voatz will soon be migrating to the SHA-3 family of hash functions on some devices.

Certificate Transparency

Certificate transparency is an emerging standard designed to be able to check or audit the certificates presented during the setup of an HTTPS connection. When any host sets up an HTTPS certificate, it is issued by what is called a Certificate Authority (CA). Certificate Transparency aims to have close to real-time monitoring to find out if a certificate has been issued maliciously or by a compromised certificate authority. When a certificate is issued, the certificate authority must submit the certificate to a number of append-only certificate logs, which can later be cross-checked by the client and scrutinized by the owner of the domain. The certificate must exist in at least two logs in order for the certificate to be valid. Details about how log proofs work are described here (https://www.certificate-transparency.org/log-proofs-work).

Certificate Pinning

To prevent Man-in-the-Middle attacks, where legitimate traffic is intercepted and altered between the voter and the voting system, the Voatz application implements certificate pinning, which checks the server's certificate against a local copy of the expected certificate. The certificates are refreshed as needed during periodic application updates.

Sanitization and Validation

Voatz implements secure programming practices based on a "design by contract" model with proper data input and output validation. Thus, if the interface says it will return a "number," it should return a number and no other characters. If the server is expecting a string of less than or equal to 24 characters, the platform ensures the interface will only return up to 24 characters. This helps prevent innocent errors and, more importantly, can reduce the likelihood of various injection and memory corruption attacks.

DDoS Attack Mitigation

Voatz protects all of its infrastructure from distributed denial of service (DDoS) attacks, which are malicious attempts to disrupt normal network connectivity by flooding the target infrastructure with illegitimate internet traffic. The Voatz platform uses a highly resilient 32-node cloud infrastructure, built across multiple service providers, including:

- Amazon Web Services - AWS (U.S.)
- Microsoft Azure (U.S.)
- Microsoft Azure (Europe)
- OVH (Canada)

Continuous DDoS mitigation involves establishing a secure perimeter around the critical infrastructure and allowing or denying certain traffic based on filters or rules. The Voatz platform takes advantage of the flexible nature of the cloud and the infrastructure is adapted defensively in the event of an attack.

The platform leverages multiple capabilities to absorb and deflect unwanted traffic. Key services employed in the DDoS attack mitigation strategy include:

DNS Redundancy

One of the most common targets of DDoS attacks is the Domain Name System (DNS). Voatz uses highly available and scalable DNS service providers designed to route users to the optimal endpoints. This approach makes it possible to manage traffic through a variety of routing types and provides additional advanced routing capabilities to protect domain names from DNS-based DDoS attacks. Voatz also uses DNSSEC to ensure the security of its DNS entries.

Multiple Points of Presence (PoPs) and Geoblocking

Voatz distributes traffic across multiple Points of Presence (PoPs) and filters requests to ensure that only valid HTTPS requests are forwarded to backend hosts. Filtering and distributing network traffic across multiple PoPs increases platform resilience and ensures legitimate traffic can reach its destination with minimal friction. The platform also utilizes geolocation restriction, known as geoblocking, which is useful for isolating attacks originating from a particular geographic location.

Web Application Firewall (WAF)

Firewalls help protect web applications from common exploits that can affect application availability, compromise security, or consume excessive resources. Depending on the type of election and threat patterns, Voatz deploys customized web security rules to control which traffic accesses which endpoints. Web security rules that target specific DDoS request patterns can be very effective for minimizing the effect of a DDoS attack.

Elastic Load Balancing (ELB)

Load balancing enables the automatic distribution of application traffic to several Voatz servers across multiple Availability Zones. This technique minimizes the risk of overloading a single server instance. Elastic Load Balancing only supports valid TCP requests, so DDoS attacks such as UDP and SYN floods are not able to reach the platform.

Appendix B: Voter Authorization and Remote Enrollment

Before voters are invited to download the Voatz app, each jurisdiction must perform voter **authorization**. While outside the scope of this paper, ensuring the integrity of the Voter Registration System is critical to the security of the election. The authorization and enrollment process is outlined step by step as follows:

1. Using their respective state's voter registration system, participating counties designate who is eligible to vote and who is authorized to mark their ballot using Voatz.
2. Voters who meet both criteria are notified of their eligibility to vote via email or letter from the jurisdiction. The correspondence provides instructions on how to configure their device to vote remotely and enrollment credentials to authenticate their identity.
3. Remote enrolled voters are invited via a notification on their smartphone to download the Voatz app, where the correct precinct ballot style is automatically delivered.
4. State election officials initiate the blockchain and instantiate verifying nodes.

The list of eligible voters, as well as the ballot styles that are sent to their smartphones, resides in each jurisdiction's Voter Registration System. Voatz partners with election officials to access the Voter Registration System, tying each voter's identity to their record to ensure they are registered before allowing them to access their ballot.[21]

Depending on the security requirements of the specific jurisdiction, Voatz can use multiple data sources and methods to verify voter identity and eligibility where required. Typical eligibility requirements include citizenship, age, address of residence, and, in some states, felon status.

For those deemed eligible, a remote enrollment invitation process then provides remote voting instructions and enrollment credentials in the form of a PIN or QR code, ensuring that, though anyone can download the Voatz application, only duly registered voters can use the application to vote.

Appendix C: Identity Proofing Process

1. Voter identity proofing begins with scanning a government-issued photo identification (ID) card. The voter uses their smartphone's camera to take a picture of their driver's license, state-issued ID, or the face-page of a U.S. passport, which the CSP then verifies the validity of.
2. The voter then captures a video self-portrait to establish identity and "liveness" through facial recognition technology.
3. Comparison of the individual from the biometric liveness test to the photo in the government-issued ID is done via secure communication between the CSP and an authorized Identity Provider (IdP) to validate the voter's identity.

Appendix D: Ballot Anonymization Process

1. The smartphone automatically notifies the state's voter registration system that the voter has submitted a ballot. (This step fulfills the state's requirement to capture voter history in order to know who submitted the ballot.)
1. The ballot's selections are counted using double-entry accounting of credits and debits, inherent to blockchain technology.
2. The ballot is anonymized, with the voter's real ID is stripped from the ballot and replaced by a unique, anonymous voter ID (AVID) to preserve voter privacy while still allowing for post-election audits.
3. Each vote is encrypted and added to the blockchain, which is redundantly distributed across 32 servers residing in highly secure cloud data centers (see Vote Storage: The Blockchain).
4. Ballot receipts are sent to both the voter and the jurisdiction to confirm the vote has been captured. Both ballot receipts are marked with the anonymous voter ID.

Appendix E: How Voatz Stores Votes Securely on the Blockchain

Voatz is built on a highly optimized and resilient, permissioned (or private) blockchain, using the IBM/Linux HyperLedger framework. Differing from public blockchains like Bitcoin, Voatz must first authorize participation by voters and auditors using 16/32 verified validating nodes, split between multiple geographically-separated cloud providers. The Voatz platform is extensible to allow Secretaries of State and State Election Boards to increase the number of nodes, as well as to designate who can participate in the blockchain network as verifiers.

Verifier nodes (or servers) function to verify the authenticity of the collection of anonymous votes sitting in "blocks" before they are added to the blockchain. Once a block is verified and added to the collection of previous blocks, the entirety of the chain, or "blockchain" ledger, containing all of the votes is copied to each verifying server and cannot be changed.

Because the blockchain ledger is transparent and distributed, validation and verification of votes is faster and more secure in the event that a recount or audit is needed. Blockchain voting is the first logical, digital step to eliminating the complexities of traditional paper ballot voting.

The mobile vote, when cast on the blockchain, is secure, distributed, synchronized, and immutable—meaning that once it is posted, it cannot be altered or deleted, and every copy of this anonymous vote is identically distributed across 32 other servers, removing any single point of failure against hacks and data corruption.

Spoiling a Ballot

Election officials can choose to enable the Voatz app to allow for the ability to change a previously recorded selection, therefore giving the voter the opportunity to change their vote up until the closing of the polls. Since the data on the blockchain is immutable, both ballots will be recorded, however, only the voter's ballot with the most recent timestamp is counted.

Appendix F: The Post-Election Audit Process

The following expands upon the features of the Voatz mobile voting platform that allow for the remote audit workflow to be conducted by a given jurisdiction:

1. When a voter receives a ballot on their smartphone, the anonymous voter ID (AVID) is generated by the smartphone to identify the voter in all voting sessions for the active election.
2. After the voter initiates a voting session, marks and reviews their ballot, and submits their ballot to the blockchain, voter credit is delivered to the jurisdiction.
3. Each vote is represented in cryptographic tokens that fully encapsulate the election, the anonymous voter ID, and the choice selected. These cryptographic tokens (votes) are randomly distributed over the blockchain servers.
4. Two automated processes, called "smart contracts," are run after ballot submission to: confirm there have been no overvotes, and determine when consensus has been reached on a complete ballot, wherein all votes from the ballot are added to the blockchain.
5. Once complete, a ballot receipt and a copy of the voter's affidavit are sent to the voter via a digitally signed email containing the election name, election date, jurisdiction name, the anonymous voter ID, and a list of all contests and choices made. An identical ballot receipt and the voter affidavit are also sent to two different mailboxes in the jurisdiction.
6. When the polls close, election staff follow the tabulation process outlined above (see Jurisdiction Tabulation), and the audit checks can be performed.

Endnotes

[1] "Number of smartphone users worldwide from 2014 to 2020." *Statista*.

[2] "U.S. Smartphone Penetration Surpassed 80 Percent in 2016." *Comscore*. 3 Feb 2017.

[3] Mearian, Lucas. "What is blockchain? The complete guide." *Computer World*. 29 January 2019.

[4] "What Is Blockchain Used For Besides Bitcoin?" *Forbes*. 17 November 2017.

[5] Yaga, Dylan et al. "Blockchain Technology Overview." *National Institute of Standards and Technology*. October 2018.

[6] Reints, Renae. "2018 Midterm Election Sets Record as the First to Exceed Voter Turnout of 100 Million People." *Fortune*. 7 November 2018.

[7] Domonoske, Camila. "A Boatload Of Ballots: Midterm Voter Turnout Hit 50-Year High." *National Public Radio*. 8 November 2018.

[8] Zetter, Kim. "The Crisis of Election Security." *New York Times*. 26 September 2018.

[9] Vine, David. "Where in the World is the US Military?" *Politico*. July/August 2015.

[10] "Americans Can Vote. Wherever They Are. 2016 Post-Election Report to Congress." *Federal Voting Assistance Program*. 2017.

[11] "DoD Releases Study of U.S. Voters Abroad." *Federal Voting Assistance Program*.

[12] Ortiz, Erik et al. "Midterms 2018: Voters Face Malfunctioning Machines and Long Lines at Polls Across Country on Election Day." *NBC News*. 6 November 2018.

[13] Schur, Lisa and Douglas Kruse. "Fact sheet: Disability and Voter Turnout in the 2016 Elections." *Rutgers School of Management and Labor Relations*.

[14] Breitenbach, Sarah. "Aging Voting Machines Cost Local, State Governments." *Pew Research Center*. 2 March 2016.

[15] "Types of Voting Equipment." *National Conference of State Legislatures*. 20 August 2018.

[16] Mobile Fact Sheet." *Pew Research Center*. 5 February 2018.

[17] Ibid.

[18] Dahlia, John. "History-making Mobile Voting App for Overseas Military Now in 24 Counties." *WV News*. 25 September 2018.

[19] "System Certification Process." *U.S. Election Assistance Commission*.

[20] "How To: Trusted Builds." *Github*. 14 July 2017.

[21] "Frequently Asked Questions." *Voatz*.