White Paper: Enhancing Democracy and Strengthening Governance Using Blockchain Technologies

ATARC Blockchain Working Group

September 2021

Contributors:

Michael Bailey, Utah State University

Lindsay Ellsworth, ATARC Blockchain Working Group Advisor Chair Gabriel Irizarry, Executive Security Architect, IBM

Bill Rockwood, ATARC Blockchain Working Group Government Chair, Congressional Staff Jim St. Clair, Chief Trust Officer, Lumedic

Eric Burger, Georgetown University

Brian Hough, Airblock Technologies

Frederic de Vaulx, Prometheus Computing

Nicole Mandes, ATARC

Advanced Technology Academic Research Center
designed by government • led by government • attended by government

Table of Contents

I. Executive Summary

The US election system has been recently subjected to unprecedented attacks on its integrity and systemic trust. While multiple social and political factors compound the difficulties noted in 2016 and 2020, the state of election technology contributed to the crises and accentuated distrust in the reliability of the world's longest democracy.

Distributed Ledger Technology, commonly called "Blockchain", is an emerging technology that is being currently utilized today within private industry, government agencies, and military branches in a variety of effective ways; it is possible that it can be used to improve our voting process to be more accessible and secure. The first blockchains were conceived as a way to avoid centralized banking in financial transactions. Examples include Bitcoin and Etherium. In the case of Etherium, additional capabilities were introduced, including basic programming logic called smart contracts. In order to avoid centralization, nodes for these networks are able to join and leave the network at will, with no central governing authority managing the network. Rather, each node merely needs to run the prescribed, open-source blockchain software, and each node competes with the others to gain the ability to post transactions to the blockchain ledger. Later blockchains diversified for other purposes and achieved other ways of managing the ability to post transactions to the blockchain ledger.

Now, blockchain systems may be based on "public" chains (such as Ethereum, Bitcoin, Microsoft ION, etc.) or "private" permissioned chains (such as Hyperledger or Corda). Both systems retain the same basic characteristics in terms of cryptographic mechanisms to encode "chains" of data, based on mathematical consensus models. Additionally, blockchains can be used both for supporting vote tabulation and to provide voting anonymity through self-sovereign identity (SSI).

The purpose of this white paper is to explore how using blockchain technology for voting in elections can benefit the United States by creating more efficient, transparent processes which increase both voter participation and overall trust in government. The integration of Blockchain based voting services has the potential to increase democratic participation in the election process. Blockchain is an enabler to mobile voting, a concept that may tremendously increase participation but has been hindered by technical auditability.

Current systems of vote tabulation also face challenges, particularly regarding transparency.

There are notable strengths and weaknesses with blockchain to support voting systems, as noted in the tables below.

Blockchain Strengths	Impact on Election Applications
They distribute trust, so that no minority cartel can arbitrarily change their contents.	Presuming the blockchain is distributed across a sufficient number of entities, collusion is very difficult to achieve to alter results.
They are an immutable record, where no existing data can be removed or changed.	Votes or blocks of votes are written sequentially to an unchangeable register, with time stamps and digital signatures. They are auditable by nature.
They can be publicly readable.	The votes are publicly accessible, but IDs are cryptographically anonymized. Chaincode can be used to hide votes until after the poll closes. Steps can be taken to provide for differential privacy.
They are redundant and fault tolerant.	A copy of the ledger is kept on each of its many nodes. It is extremely unlikely that a database-type crash can lose votes or other data. A comparison of a random set of nodes can confirm the authenticity of the vote.
They require cooperation of diverse, often competing entities.	Entities who are concerned about election integrity can apply to run a permissioned node. Care must be taken to diversify interest groups to prevent collusion.

Blockchain Weaknesses	Impact on Election Applications
Writes to blockchain are relatively slow and resource intensive, requiring more resources than other database types do.	Initially, more resources are required based on blockchain's computational and network communication intensity compared to today's centralized databases. However, as blockchain technologies advance with time and use, we expect new efficiencies to emerge.

There are a few precursors to deploying a blockchain voting initiative. These include having the authority to undertake such efforts and then getting funding for the research and development of blockchain voting projects. We foresee two ways in which this can occur: passing legislation and using the federal appropriations process to create an incremental record.

This proposal focuses on pursuing incremental wins within the appropriations process to create a sense of momentum and a transparent track record of success for blockchain voting initiatives. With emerging

technologies, these can usually be done in a three-step (or multiple year) appropriation submission where:

(1) An acknowledgment that an emerging technology could be used to assist with a problem;

(2) A report/feasibility analysis or pilot program is used to consider the issue in more detail; and

(3) Funding is allocated for the development and deployment of the project.

We propose an appropriation approach to advancing e-voting systems through applications of blockchain technologies.

II. Enhancing Democracy with Blockchain Technology

Confidence in Elections is Vital to Democracy

Elections are a foundational component and vital cornerstone of American democracy. "The American public's confidence that their vote counts - and is counted correctly -- relies on secure election infrastructure" -Kirstjen Nielsen, Secretary of Homeland Security (2017-2019) According to Pew Research Center, only around 24% of Americans trust the government to do the right thing almost "always or most" of the time.[1] Additionally, the US is challenged by declining participation in the election system. In 1968, 74.3% of the American population was registered to vote. That percentage has declined quite consistently over the past 50 years and in 2016, only 64.2% of our population was registered to vote. While our population grows larger, the number of registered voters continues to decrease.

Voting Accessibility

Remote Voting. For the purposes of this white paper and future projects, we will focus on the use of blockchain for the enablement of voting remotely via a secure mobile application (app). A mobile voting solution would not only enable voting accessibility for those with a physical or mental impairment, it would also allow for a more secure voting method for deployed service members who currently rely on mail-in voting.

Use Case: Remote Voting for Service Members

Service members stationed abroad face impediments to voting. There are many initiatives to increase active duty service members' voting participation. For example, by law (the MOVE Act), all states must allow service members to remotely request absentee ballots, and today all states do this over the Internet.

This ability to request absentee ballots literally anywhere in the world is far superior to prior systems where overseas voters had to physically go to a consulate, a major base, or write for ballot materials. However, it has two serious issues not present in domestic absentee ballot systems. Domestic mail

[1] Public Trust in Government: 1958-2021

normally takes under a week for delivery. Conversely, because of foreign mail systems and often the reliance on FPO or APO forwarding, it can take weeks for a paper ballot to reach a deployed service member. And, correspondingly, it can take weeks for the filled-in ballot to make its way back to the state election officials for certification and counting. This long delay means many service members' ballots never get counted because the ballot arrives well after the election is over. The MOVE Act streamlined the ballot request process. The good news is it greatly improved the voting rates, from under 50% to over 80%.

However, that means that close to 20% of eligible service members still could not have their vote counted due to delays in sending paper ballots around in the field.

While a possible solution to this is e-voting, the computer science, government, and security community are almost unanimous on the opinion that electronic voting is fraught with risks, with the result that to date the most secure voting systems are mark-sense paper ballots: electronic tabulation with a paper trail. However, those studies do not take into account the unique hurdles service members face when voting. In this case, more especially as we are talking about approximately 0.5% of the voting population, the potential risks of electronic voting are offset by the known loss of franchise for our service members.

Use Case: Enhancing Voting Opportunities for the Disabled

Over one in four adults in the United States has some type of disability - this is over 61 million people.[2] "Although voting accessibility has improved since the Help America Vote Act (HAVA), people with disabilities register and vote at lower rates than other Americans and face unique challenges at the polls."[3] U.S. election systems and infrastructure are not designed with disabled voters in mind. Disabled voters' unique and varying needs are frequently overlooked by policymakers, and election accessibility is sometimes dismissed as a logistical and fiscal impossibility. Voting options that could dramatically improve accessibility are too often sacrificed in the interest of security. The result is inaccessible polling places and voter registration offices; inadequate registration and voting accommodations; and election information that is unreadable for some."[4] According to a 2017 report by the U.S. Government Accountability, "Voters with Disabilities: Observations on Polling Place Accessibility and Related Federal Guidance," roughly two-thirds of the examined polling places had at least one potential barrier such as lack of accessible parking, poor paths to the building, steep ramps, or lack of a clear path to the voting area. Although most polling places had at least one accessible voting system, roughly one-third had a voting station that did not afford an opportunity for a private and independent vote."[5]

> **DISABILITY DEFINITION:** Under the ADA, an individual with a disability is a person who has a physical or mental impairment that limits one or more major life activities along with a record of such impairment, or is regarded as having such an impairment.
>
> **PHYSICAL IMPAIRMENT:** A physical impairment is defined by the ADA as: "any physiological disorder, or condition, cosmetic disfigurement, or anatomical loss affecting one or more of the

[2] Disability Impacts All of Us Infographic
[3] Accessible Voting Technology Initiative; Defining the Barriers to Political Participation for Individuals with Disabilities
[4] Enhancing Accessibility – US Elections
[5] Election Blocked from the Ballot Box: People with Disabilities by Elizabeth Pendo

following body system: neurological, musculoskeletal, special sense organs, respiratory (including speech organs), cardiovascular, reproductive, digestive, genitourinary, hemic and lymphatic, skin, and endocrine."

“As a Voter with a Disability, you have the right to:

- Vote privately and independently
- Have an accessible polling place with voting machines for voters with disabilities you may either:
- Seek assistance from workers at the polling place who have been trained to use the accessible voting machine, or
- Bring someone to help you vote

You may request your local election officials to tell you about any voting aids, voting assistance, and absentee ballot procedures that are available.”[6]

An estimated 7 million voters have a vision disability.[7] In 2020, mail-ballots offered both disabled and nondisabled voters a safer alternative to voting at the polls, but presented complications to those with visual and dexterity impairments. Assistive technologies for the blind and vision impaired such as JAWS and Kurzwell Education offer an array of useful features including screen readers, which are available in multiple languages and dialects. These are also helpful for those who are nonnative English speakers.

In addition to blind voters, blockchain enabled electronic voting systems will be of assistance to voters with mobility disabilities which make it difficult for them to physically access their precinct. These assistive technologies are available on mobile devices which can be integrated and enhanced using blockchain.

III. About Blockchain: Beneficial Characteristics for Election Systems

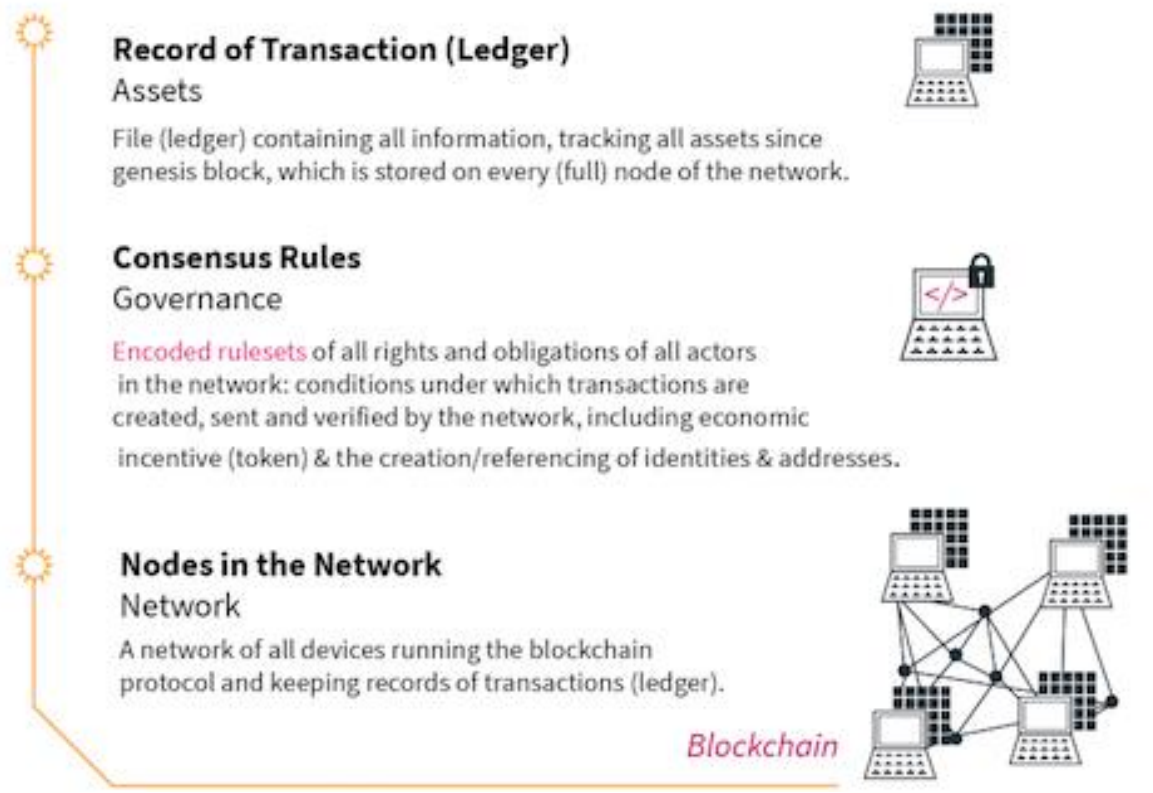
In the broadest sense, blockchains are distributed, immutable ledgers. A ledger is a store of transactional data. They may be thought of as a specialized database, which many are familiar with. This combination of distributed, immutable attributes makes blockchains uniquely suited to election technologies.

The difference for blockchains lies in the descriptive modifiers: “distributed”, and “immutable”.

- Distributed, meaning that there are many copies of the ledger in separate servers or “nodes”, scattered across geographies, organizations or other dimensions. Each of these copies is maintained and updated by its own node in accordance with agreed-upon rules, such as consensus between nodes as to the validity of the transaction.

[6] Home Voters Voting Accessibility
[7] Enhancing Accessibility in US Elections

- Immutable, meaning that ideally data once written to the ledger can never be changed, enforced by the very design of the ledger. While nothing is really unchanging, a properly designed blockchain will be extremely difficult to change without it being publicly noticed.



Source: the book "Token Economy" by Shermin Voshmgir, 2019

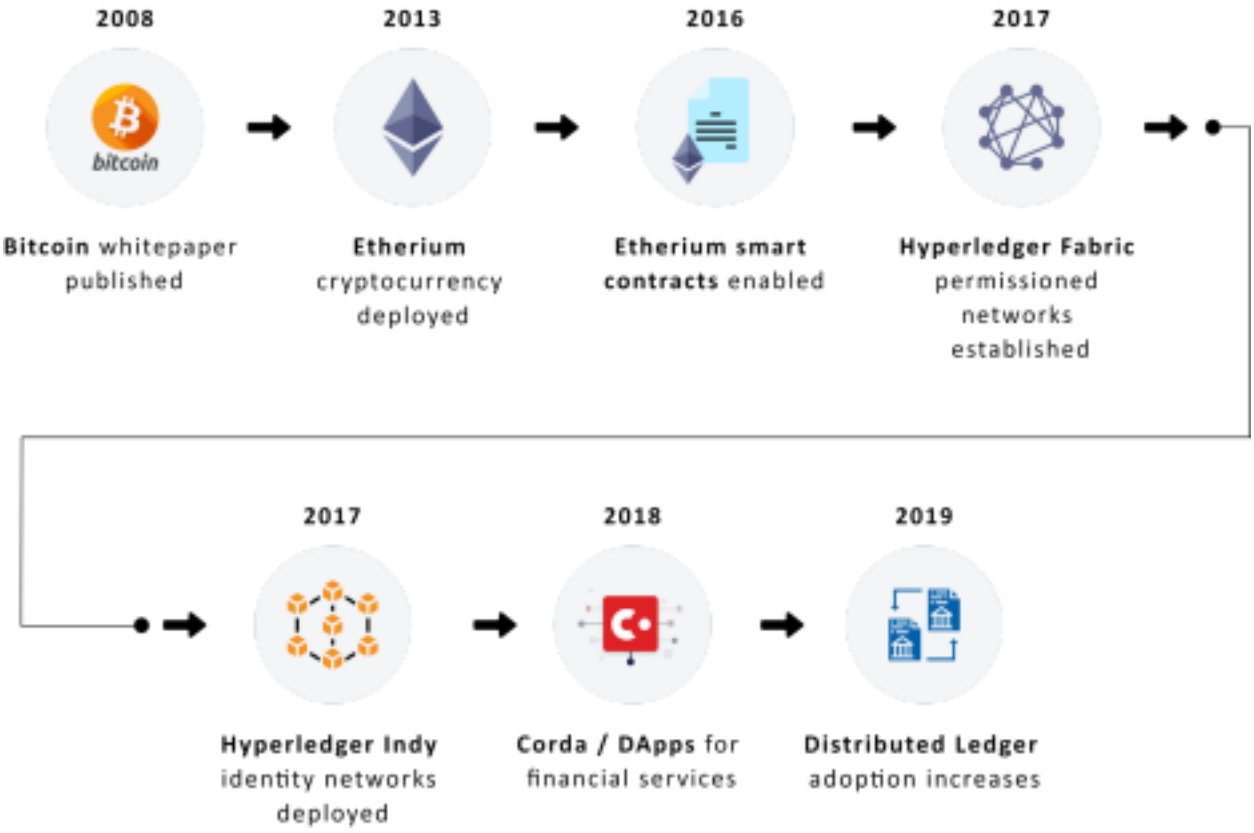
A simple model for blockchain technology is a ledger built on a foundation of consensus rules running on network compute nodes, as shown above. Different types of blockchains are determined by the consensus rules that are implemented in the blockchain software.

A Brief History

The first blockchains were conceived as a way to avoid centralized banking in financial transactions and solve the electronic transaction problem of "double spend". Examples include Bitcoin and Etherium. In the case of Etherium, additional capabilities were introduced, including basic smart contracts. In order to avoid centralization, nodes for these networks are able to join and leave the network at will, with no central governing authority managing the network. Rather, each node merely needs to run the prescribed, open-source blockchain software, and each node competes with the others to gain the ability to post transactions to the blockchain ledger.

Later blockchains diversified for other purposes, and achieved other ways of managing the ability to post transactions to the blockchain ledger. Smart contracts were further developed, and permissioned

networks emerged, where transactions are posted according to voting mechanisms limited to a defined set of "permissioned" nodes - nodes with permission to either write to the blockchain or read from it. Notable among these are those developed by the Linux Foundation's Hyperledger project, such as Fabric, and the R3 Consortium, with Corda.



Source: Paramount Software Solutions, Inc.

Types of Blockchain

There are different types of blockchain:

Permissionless and public blockchain:

In a permissionless blockchain, any entity is able to propose new blocks to the blockchain to be validated. This is done through the entity adding a node to the blockchain and competing to gain the privilege to propose a new block (e.g. by being the first to complete a computation). The other nodes on the blockchain examine the proposed block against a set of criteria including its sources, content, syntax, and digital signatures. A majority of the nodes on the blockchain (sometimes over ⅔) must agree that the proposed block is valid before it is finally added to the ledger. Being a public blockchain enables anybody to read data from the ledger.

Permissioned and public blockchain:

In a permissioned blockchain, not every entity is allowed to propose blocks to the blockchain. Nodes need to be authorized to participate on the blockchain network. For these networks, the competition step used by permissionless blockchains is skipped, and instead a transaction is written as soon as the required majority of the nodes agree that the transaction is valid. Being a public blockchain enables anybody to read data from the ledger.

Permissioned and private blockchain:

This type of blockchain shares the permissioned attributes described in the preceding section. However, as a private blockchain, not everybody is allowed to access and read the data on the ledger. In some cases, an API is provided to allow selected disclosure of ledger data

Nodes in blockchains can be hosted by a single entity, or by many. To achieve the desired levels of trust that elections require, many diverse, competing entities are the best hosts for a blockchain, whether it be permissioned or permissionless. Because of the overhead of computational competitions, many permissionless blockchains are slow and, by design, consume a lot of resources.

Combining the attributes desired for election systems (transparency, node diversity, efficiency), arguably the type of blockchain most suited to this purpose is a permissioned, public blockchain with many nodes, each hosted by an independent entity, where the voter identity is never retrievable (anonymized), their vote is not visible until after the election closes, and a reasonable level of differential privacy can be assured.

IV. Proposal

The ultimate success of a blockchain voting initiative will hinge on an incremental approach and targeted application for areas where it can be helpful.

The timeframe for deployment and the extent to which blockchain may be used for elections remains an open question, but there are targeted applications to which blockchain can be successfully deployed in the short-term. If such projects are successful, it creates a more compelling narrative for wider deployment over the longer terms. This proposal breaks things down into a phase-based approach and identifies areas where the government could logically start exploring blockchain and voting initiatives; namely, voting access for individuals with disabilities and voting access for service members stationed abroad.

Our Desired Outcome:

There are a few precursors to having a blockchain and voting initiative to be deployed. These include having the authority to undertake such efforts and then getting funding for the research and development of blockchain voting projects. There are two ways in which this can occur: passing legislation, and using the federal appropriations process to create an incremental record.

This proposal supports the idea of introducing and passing legislation. Legislation will be an aspect of the solution in the future. However, this is often a lengthy process that involves many political obstacles. When a fundamental American value like voting is involved, the political stakes and degrees of trust

required before a new approach is considered is heightened.

Instead, this proposal focuses on pursuing incremental wins within the appropriations process to create a sense of momentum and a track record of success for blockchain and voting initiatives. With emerging technologies, these can usually be done in a three-step (or multiple year) appropriation submission where: (1) an acknowledgment that an emerging technology could be used to assist with a problem; (2) a report/feasibility analysis or pilot program is used to consider the issue in more detail; and (3) funding is allocated for the development and deployment of the project. These can occur in a single appropriations submission or over the course of a few years.

This proposal is to deploy this strategy in two areas in which blockchain and voting can be most strategically used: to assist voting access for those with disabilities and for service members stations abroad. If these endeavours prove successful, a wider use for blockchain and voting can be further explored in the future.

In the current cycle, this is the proposal language that we are advocating for:

Request #__ (BLOCKING & VOTING for Individuals with Disabilities)

TITLE II — DEPARTMENT OF HEALTH AND HUMAN SERVICES — ADMINISTRATION FOR COMMUNITY LIVING

Emerging Technology Voting Access for Individuals with Disabilities.-- The Committee recommends $8,463,000 for Voting Access for Individuals with Disabilities program, which is $1,000,000 above the fiscal year 2020 enacted level and the fiscal year 2021 budget request. The Voting Access for Individuals with Disabilities program authorized by the Help America Vote Act provides formula grants to ensure full participation in the electoral process for individuals with disabilities, including registering to vote, accessing polling places, and casting a vote. Furthermore, the Committee notes the potential of emerging technologies, like distributed ledger technologies or blockchain, to engage greater voting access for individuals with disabilities. The Committee recommends that a feasibility analysis into the use of emerging technologies to assist with voting access for individuals with disabilities, that includes but is not limited to, the particular voting challenges faced by individuals with disabilities, how emerging technologies could be unitized, the challenges of such a system, and the base requirements such remoting system may entail.

Request #__ (BLOCKING & VOTING for Service Members Stationed Abroad)

Research, development, test and evaluation – DEFENSE-WIDE

Voting Access for Service Members Stationed Abroad.—The Committee commends the prior work the Secretary has done to provide military postal service support to United States citizens living in overseas locations and employed by the North Atlantic Treaty Organization (NATO), if such citizens perform functions in support of the Armed Forces of the United States. However, given the importance of voting in US elections, the logistics of mail-in voting is time consuming and present many barriers that likely reduce voting access for service members stationed abroad.

Furthermore, the Committee notes the potential of emerging technologies, like distributed

ledger technologies or blockchain, to engage greater voting access for servicemembers stationed abroad. The committees the Under Secretary of Defense for Research and Engineering is directed to prepare a report on the use improved voting access for servicemembers stationed abroad. This report should include, but is not limited to, the voting challenges faced by overseas servicemembers, how emerging technologies could be unitized, the challenges of such a system, and the base requirements such remote voting system would entail. This report is to be made available on the Commission website with 270 days of the date of enactment of this act.

Model Blockchain:

As expressed earlier in this document, the voting ecosystem and process is very complex, with many moving parts to enable voters to take part in their civic duty even if they have disabilities or are not in their voting location during the voting period. The ecosystem can be decomposed

into components and processes that each have their own complexity and risks. For instance voter registries can be considered critical components as they are used to verify that an individual is eligible to vote. They are decentralized, implemented and maintained in different ways, and subject to different regulations. The ballot is another critical component as it lists the candidate items that a voter has to vote on and records the choice of the voter. In this section we break out three components that can be addressed in phases using blockchain technology.

Proposed Phases

1. **Tabulation**

   In this section we examine the tabulation component of the voting ecosystem. Tabulation is the process of totaling the votes. As with the two other components, it is a decentralized process, as it is managed at the state and local levels. However, the counting of the ballots and the aggregation of the results must be done in a trusted manner so that people have confidence that every eligible ballot was processed and the result is fair. Things get more complicated when ballots are not just collected in person during the voting period. Increasingly there are also mail-in ballots, provisional ballots and UOCAVA ballots (Uniformed and Overseas Citizens Absentee Voting Act), which makes the tabulation more complex and prone to errors.

   As with voter registries and ballot submission, ballot tabulation can benefit from the use of blockchain based solutions. Every time a ballot is processed, a transaction can be added to a blockchain ledger to record that a ballot was processed at a given location, a given time, by a given machine or process. Based on the practices and rules of states and local jurisdictions, decisions would be made to count a ballot or not. The logic used as well as the decisions made for each step can also be recorded in the ledger to have a transparent record of the processes, steps and decisions taken during tabulation. This will require an analysis of what processes, steps and data should be logged to represent an accurate observation of what happened. In addition, part of the logic can also be encoded into smart contracts to not only make the data state changes transparent but also their execution. This solution can be integrated into the current voting ecosystem, not replacing existing hardware solutions, rather enhancing these solutions, providing a decentralized network of trusted logs that record what happens during

ballot tabulation. This will bring consistency across the different jurisdictions while maintaining localized rules and solutions.

2. SSI Voter Identification

Self-Sovereign Identity (SSI) is the collective reference to the concept, policies and architecture to instantiate individual ownership of identity - identity is "sovereign" to the individual who exercises ultimate authority as to how it's shared. For the purposes of this document, SSI is a set of technologies that build upon core concepts in identity management, distributed computing, blockchain or distributed ledger technology (DLT), and cryptography.

Applying the principles of SSI to voting potentially addresses some of the challenges noted in traditional paper ballots and electronic voting. While every system requires multiple components to operate correctly, especially governance and regulation, SSI in voting can specifically mitigate certain vulnerabilities in the voting process:

- SSI provides cryptographic trust that supports the underlying premise of "one person, one vote" without demanding multiple verifications or proof of identity ● SSI removes the need for real-time involvement of a centralized identity authority in the voting process, since a self-contained voter ID will be in the possession of the voter.

- It precludes the creation of multiple identities that can confuse or disrupt the compilation and tabulation of electronic votes.

- An SSI credential that is cryptographically signed by a trusted authority is far more authoritative and counterfeit resistant than even the best paper credential (i.e. driver's license).

The following table highlights the principles of SSI mapped to voting requirements.

SSI Mapped to Voting Requirements

From "*Open democracy, voting & SSI*" by Shannon Appelcline

- Authenticity – a voter must be able to prove an identity.
- Accreditation – a voter must be able to prove they have a right to vote.
- Non-repudiation – a voter must not be able to change a vote after lock-in
- Immutability – an attacker must not be able to change a vote.
- Auditability – a state must be able to recount votes and verify their authenticity, accreditation, non-repudiation, and immutability.

Accessibility

- Openness. A voter must be able to vote in a time, place, and manner that maximizes his likelihood of voting.
- Simplicity. A vote must be able to vote without undue complexities or burdens.

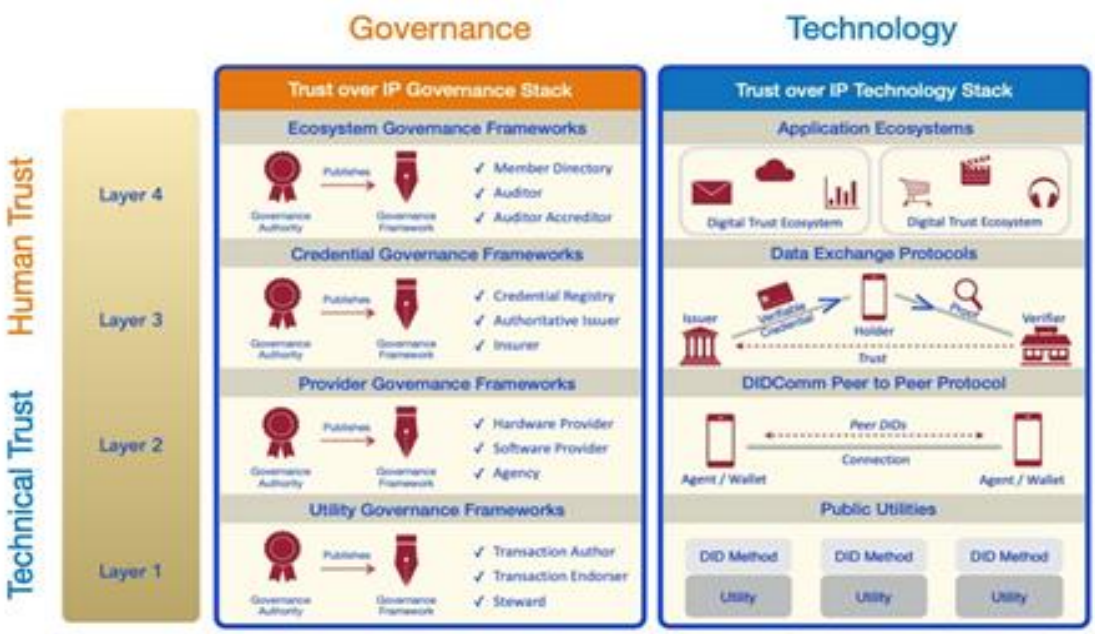
It can be seen that SSI credentials held by voters on widely available smartphones will support superior election methodologies. While smartphone access cannot be a required precondition for voting, where they are available, they can make use of blockchain technologies to facilitate the voting process.

3. e-Vote using Blockchain and Public Key Infrastructure (PKI)

Per the Executive Order on Improving the Nation's Cybersecurity, the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. Using blockchain for voting helps ensure trust between the public and the government. In addition, by using smart contracts to automate the tallying of votes, voting becomes a much more secure and cost-effective process. Implementing the application with a Hyperledger Fabric web app decreases the chance of election fraud and enhances the voting solution by using blockchain technology.

The proposed solution is based on open standards and on a complete architecture for Internet-scale transitive trust that integrates cryptographic verifiability at the technical machine layer with human trust at the business, social, and legal layers.

Interoperability of the Blockchain eVote solution, provides the necessary links between governance and technology.



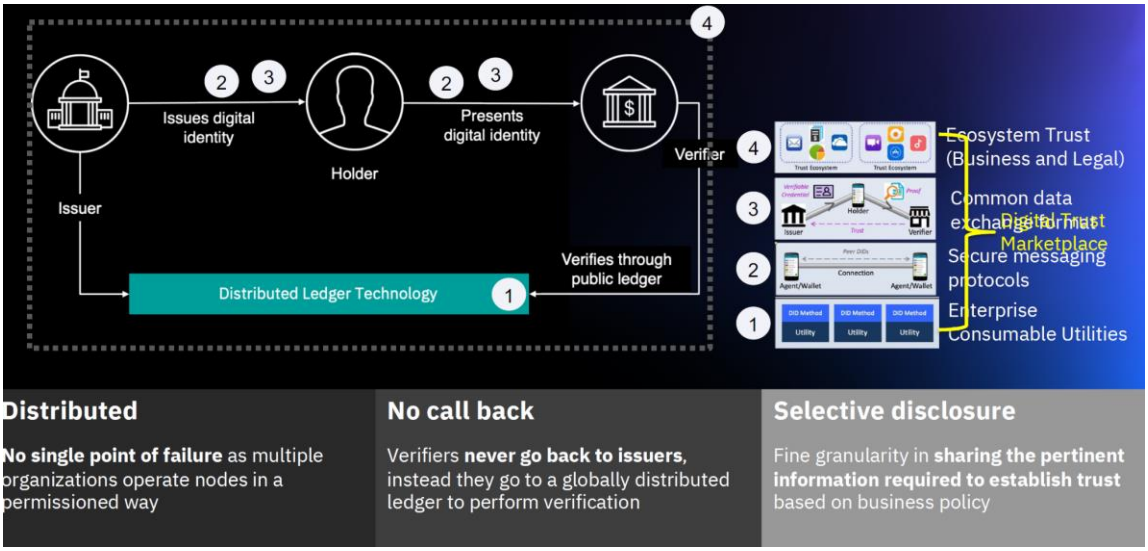
Source: Trust Over IP Foundation

For a demonstration project, the voting process starts with the user registering to vote by providing their government-approved ID, registrar district, and first and last name. In this step, we can check to see if the ID is valid and has not been registered previously. We recognize this will not be sufficient for a live deployment, as these data elements are all discoverable in the

public domain. For a live deployment, we can use a certification authority, such as the employer (DoD, in this case), or tie to a validation based on the service member's Common Access Card (a smart card). If all validates, the user's wallet creates a private and public key for the voter. Our certificate authority that is running on the cloud validates the public key and places it in the user's wallet for the user's use.

After that, the voter uses the credential from their wallet to generate a unique, one-time identifier to submit their vote, during which the application checks if this voter has voted before and tells the user they have already submitted a vote if so. Depending on the rules of the jurisdiction of the vote, the voter can be asked if they wish to change their vote or the voter is informed they have already voted. Note that if the jurisdiction allows voters to change their votes, the blockchain will record all of the voter's votes - it is only the last vote the voter casts before the close of the election that would be counted.

Every transaction is recorded on the blockchain and the blockchain participants reach consensus on the network, making the transaction immutable. A one-way hash of the unique one-time identifier is used to assure that the voter who cast the vote is anonymous, but that the voter themself can validate the correct recording of their vote on the ledger. We acknowledge this does not provide perfect anonymity, as characteristics of the transaction, such as when the vote was cast may leak the identity of the voter. However, salting the hash makes reidentification of the voter by correlating other uses of their self-sovereign identity much harder.



Source: IBM

Supply Chain Risk Management for the proposed solution

ATARC will require a third-party assessment team that will review suppliers for the required privacy, cybersecurity, and risk management protocols to protect the U.S. Federal Government agencies and ATARC interests. The process will include verification of the supplier's security, risk-ranking, security assessments, privacy and risk program, and over-arching cybersecurity terms.

V. Conclusions

The underlying premise of voting - “one person, one vote” - has remained unchanged since the founding of our republic. This white paper lays out a proposal to use emerging technologies, in particular blockchain, to enhance and extend our ability to deliver on this goal. This will be done by increasing access to the polls for some groups that are vulnerable to disenfranchisement, namely deployed service members and disabled Americans.

These avenues were identified as compelling and less controversial entry points for the exploration of the use of blockchain technologies for voting purposes. Under the strategy of incremental adoption, this paper offers sample language for the federal appropriations process, which, if adopted, would serve as a starting point for the funding and development of blockchain and voting pilot programs or further research and development. If these projects prove successful, it becomes much more likely that blockchain and voting initiatives will be considered for potential wider implementation.

In addition, the proposals have the potential to actually increase confidence in elections generally through improved voter identification and authentication, and through a trusted audit system. Blockchain is an enabler to mobile voting, a concept that may tremendously increase participation but has been hindered by technical auditability previously.

Blockchain technologies have the potential to assist and add value to the democratic process. It can benefit the United States by creating more efficient, transparent processes, with the potential to increase democratic participation and further trust in the election process. Ultimately, the promise of these benefits argue strongly in favor of further exploration of blockchain technology for voting purposes. This paper offers one path in which these prospects could be pushed closer to reality. One of the great promises of emerging technologies is that it can address old challenges with new solutions; but only time will tell how this story unfolds.

Definitions

Bitcoin: a digital currency created for use in peer-to-peer online transactions.

Blockchain: (from Wikipedia) A blockchain is a growing list of records, called *blocks*, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Corda: a multi-party application development platform developed by R3 that enables businesses, specifically in the industries of banking, capital markets, trade finance, insurance and beyond, to transact directly and in strict privacy using smart contracts with the open-source proprietary distributed ledger, Corda.

Cryptanalysis: the solving of cryptograms or cryptographic systems. Cryptanalysis is the theory of solving cryptograms or cryptographic systems, as well as the art of devising methods for such cryptanalysis.

Cryptocurrency: any form of currency that exists only digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

Cryptography: the processes and methods for enciphering and deciphering messages sent in secret code or ciphers.

Cryptogram: a figure, representation, or communication with a hidden significance, either by way of cipher or code.

DApps: decentralized applications, aka DApps, are software systems or technical solutions that run on a distributed computing system, such as a public blockchain or decentralized network. Such applications typically run on smart contracts and rely on blockchain or distributed ledger technology as their supporting infrastructure.

Decentralization: the dispersion or distribution of functions or powers. Specifically, in government and governance, decentralization denotes the delegation of power from a central authority to regional or local authorities, often referred to as nodes.

Ethereum: a leading decentralized, open-source blockchain network that is powered by smart contracts and which hosts the Ether token. Ethereum is considered to be the most actively used blockchain globally.

Immutability: a state of being unable to be deleted, modified, or altered. In programming and computation, an immutable object is one whose state is unable to be altered once it is created or built.

An antonym of immutability is mutability, which means the state can be altered after it is created or built.

Hyperledger: a multi-project open-source collaborative effort hosted and administered by The Linux Foundation designed to amplify, develop, and accelerate blockchain technologies.

Hyperledger Fabric: a foundational blockchain network for developing decentralized applications, software, or solutions using modern architecture.

Hyperledger Indy: a distributed ledger technology designed for decentralized identification use-cases using transferable, private, and secure credentials within the immutable system.

Mining: the technical process validating proof-of-work consensus where computer systems "mine" or "hash" data sent onto the blockchain and validate the chain in exchange for a reward for running the protocol.

Node: one of the (many) validators of a blockchain network which helps to decentralize the data and compute power of the network.

Public Key Infrastructure (PKI): the procedures and associated policies, roles, software, hardware, etc. that are used to create and use X.509 certificates such as are widely used on the web to make secure connections to web pages of trusted organizations. These certificates contain cryptographic public keys that are tied to a specific organization, and are attested to by a certificate authority.

Smart Contract: a computer program, software program, or protocol designed to automatically ingest, control, execute, or identify events, actions, or requirements of a contract or agreement.

SSI: Self-Sovereign Identity is a system where members of the system generate, control, or hold cryptologically verifiable credentials which are decentralized ways to verify and validate identity.

Special Acknowledgements

Franck Nouyrigat: Co-founder, Electis.io and previous founder of Startup Weekend

Gilles Mentré: Co-founder, Electis.io - was a special advisor to President Sarkozy of France

Nimit Sawhney: CEO, Voatz

Anthony Day: IBM Blockchain expert and author of Blockchain Won't Save the World

Pete Martin: CEO, Votem

Yolanda Robinson Darricarrere: Technologist | Federal Enterprise IT | Infopreneur | Global Cyber Policy & Law

Tom McDonough: Neighborhood Business Manager at City of Boston Mayor's Office of Economic Development

Jake Braun: Executive Director- University of Chicago's Cyber Policy Initiative | Co-founder of the DEF CON Voting Machine Hacking Village, hosted annually at DEF CON, the largest hacking conference in the world., CEO of Cambridge Global Advisors

Cecil (CJ) John: Author of the Social Currency | CEO of VirtualDeveloper.com, LLC, a Microsoft Managed Partner

Kenneth Garofalo: CEO, Block Relations

Appendix

The ATARC Blockchain Working Group conducted a multi-week speaker series to discuss the current voting process and showcase the work being done in and around the space of e-voting, particularly in relation to blockchain technologies. Presenters were selected from among the industry and government proponents of e-voting systems. Salient points raised by presenters in the series include:

- Election Infrastructure Cyber Risk Assessment. When it comes to cybersecurity and fraud risks, two of the most vulnerable points of the voting infrastructure are the voter registration databases and the websites used to display election results and information regarding voting instructions. 98% of the 8,000 jurisdictions do not have cybersecurity personnel to manage their data. By storing this data in clouds, those entities would have the resources to secure the data and use the best tech available including blockchain, which is only one piece of the solution. With voter registration databases being one of the highest value targets in the election infrastructure, blockchain makes a lot of sense to secure these. It's virtually impossible to keep someone from hacking a website. So much havoc can be done to the voter registration database by deleting the voters or changing things around. It provides a very lucrative target for the attackers. In the case of Russia in 2016, hackers actually did access the voter registration databases. The way they got in was by hacking the websites of election officials using a very simple SQL injection attack. In the last 2 presidential elections in fact websites and the databases were attacked in this manner.

- In many cases, overseas voters currently vote via email which is insecure and doesn't protect the voter at all. At DEF CON, they were able to hack these emails, among other voting methods, within minutes. For those folks already voting in these incredibly insecure ways, there must be a better option. One thing that needs to happen is there at least needs to be a paper print-out so that there's a paper back up. An open source system is needed so that the good guys can look at the technology instead of just the hackers and bad guys which is all that can look at it now. DEF CON 2 7 Voting Machine Hacking Village

- Over 100 million people used mail in voting in the 2020 election. Mail in voting is an arduous process. Many of our guest speakers had issues with voting by mail and one was completely unable to complete the process. Issues included name misspellings, lost ballots and privacy concerns.

- Standardization: We have close to 4,000 jurisdictions and don't have a standardized paper ballot. A common data format and simplified form of communication would help to streamline the entire process.

- Better contingency plans are needed for instances of natural disasters and other emergency situations. Postponing the election is the last thing we want to occur, and the mobile infrastructure is probably going to be the first to come back online. It seems there is a need for multiple facets of voting to be available via mobile so when the unexpected happens, we are ready for it.

- Example application from guest speaker: Votem: CastIron Mobile Voting Platform
- Resource: Blockchain and Election Security Webinar
- Resource: Blockchain Playbook for Federal Government
- Tabulation and Reporting Risk Resource: Election Results Reporting: Risks and Mitigations

In addition to commercial applications of blockchain technologies, example applications of blockchain are increasingly easy to find in the government. One day, perhaps blockchain enabled e-voting will join applications such as these.

- Data Foundation's Bringing Blockchain Into Government: A Path Forward for Creating Effective Federal Blockchain Initiatives (2019)
- USPS blockchain initiatives, resources and references:
    - United States Patent and Trademark Office
    - CaseMail On-Demand Postal and E-Doc Delivery and Verification)
    - CaseMail: Epostal Services
- "Permissioned blockchain networks can help reconcile the fundamental tension between the benefits of cross-industry data with the need to keep private, proprietary information private. It also has the power to illuminate supply chain risks." How the FDA is piloting blockchain for the pharmaceutical supply chain - Blockchain Pulse
- "According to Frank Yiannas, Deputy FDA Commissioner for Food Policy and Response, blockchain "has enabled food system stakeholders to imagine being able to have full end-to-end traceability. An ability to deliver accurate, real-time information about food, how it's produced, and how it flows from farm to table is a game-changer for food safety." The FDA identifies a lack of traceability as the Achilles heel of the U.S. food system. Currently, tracking data remains largely paper-based. With an eye toward updating the system, the blueprint draws inspiration from real-time tracking of aircraft, ride sharing vehicles, and delivery trucks used by companies like FedEx, Uber, and Amazon." Blockchain and the FDA's Blueprint for a New Era of Smarter Food Safety | Stanford Law School
- US Health Department Chief Discloses Functioning Blockchain Project To Track Covid-19