CAN BLOCKCHAIN IMPROVE ELECTION SECURITY?

A COMPARATIVE ANALYSIS OF EMERGING BLOCKCHAIN E-VOTING SYSTEMS

JULIA MADISON JAKUS

BOĞAZİÇİ UNIVERSITY

2022

CAN BLOCKCHAIN IMPROVE ELECTION SECURITY? A COMPARATIVE ANALYSIS OF EMERGING BLOCKCHAIN E-VOTING SYSTEMS

Thesis submitted to the

Institute for Graduate Studies in Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

International Relations: Turkey, Europe and the Middle East

by

Julia Madison Jakus

Boğaziçi University

2022

DECLARATION OF ORIGINALITY

I, Julia Madison Jakus, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature …….....

Date …….....

ABSTRACT

Can Blockchain Improve Election Security?

A Comparative Analysis of Emerging Blockchain E-Voting Systems

This research investigates whether blockchain can improve election security by increasing transparency in the electoral cycle's voting and vote tabulation phases. Statistically declining perceptions of trust in electoral institutions, rising populist rhetoric, and deepening polarization are stress-testing democratic infrastructure to the extent that a worldwide exploration for more viable alternative voting methods is underway. Although emerging blockchain e-voting systems may be the indirect product of contemporary electoral insecurity, it is another question whether they are ready for full-scale implementation. Thus, this manuscript qualitatively investigates and compares five ongoing projects worldwide based in Estonia, Russia, Switzerland, Japan, and the United States. What unique opportunity costs and policy voids surround these emerging technological infrastructures and their data management systems? Each pilot project is reviewed with a nod to the Cybersecurity Framework (CSF) Election Security Profile developed by the National Institute of Standards and Technology (NIST) and the Election Security Framework (ESF) standards.

ÖZET

Blokzincir Seçim Güvenliğini Artırabilir mi?

Gelişen Blockzincir E-Oylama Sistemlerinin Karşılaştırmalı Bir Analizi

Bu araştırma, blokzincirin seçim döngüsünün oylama aşamalarında şeffaflığı artırarak seçim güvenliğini iyileştirip iyileştiremeyeceğini araştırıyor. Seçim kurumlarına duyulan güvenin azalması, yükselen popülist retorik ve derinleşen kutuplaşma demokratik altyapıyı strese sokuyor ve bununla ilgili olarak dünya çapında daha uygulanabilir alternatif oylama yöntemleri için araştırma yürütülüyor. Ortaya çıkan blokzincir ve e-oylama sistemleri, çağdaş seçim güvensizliğinin dolaylı ürünü olsa da, tam ölçekli uygulamaya hazır olup olmadıkları başka bir sorudur. Bu nedenle, bu metin dünya çapında Estonya, Rusya, İsviçre, Japonya ve Amerika Birleşik Devletleri'nde devam eden beş projeyi niteliksel olarak araştırıyor ve karşılaştırıyor. Ortaya çıkan bu teknolojik altyapıları ve veri yönetim sistemlerini çevreleyen benzersiz fırsat maliyetleri ve politika boşlukları nelerdir? Her pilot proje, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilen Siber Güvenlik Çerçevesi (CSF) Seçim Güvenliği Profili ve Seçim Güvenliği Çerçevesi (ESF) standartları dikkate alınarak gözden geçirilmektedir.

ACKNOWLEDGMENTS

I would like to extend my sincere thanks to my thesis advisor, Dr. Zeynep Kadirbeyoğlu, for her continued patience, support, and insight throughout the research and writing of this thesis as well as to my committee members, Assist. Prof. Mert Arslanalp and Assoc. Prof. H. Akın Ünver for their insights and to Aslı Orhon for her above-and-beyond administrative efforts.

I'd also like to take a special moment to appreciate all those who have supported this manuscript by reviewing it with an open mind and, of course, to the 2019 MIR cohort, who have been a source of continued friendship, inspiration, and community. Your friendship means the world to me, and I am grateful to be forever learning from you all.

I would also like to express my deepest gratitude to all those who have dedicated themselves to sharing their pursuit of knowledge with myself, my peers, and future scholars despite the onset of the coronavirus pandemic, uncertain times at Boğazçi University, and other dimensions of academic risk in Turkey. Your bravery is not unnoticed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

THE CRISIS OF VOTING SYSTEMS

An elderly man sits alone in an oval room. He pouts out his lips. Satisfied or dissatisfied, his expression appears unchanged, but this October night dissatisfies him. He stands up from a high-backed black leather chair and carries his musing over toward the window. Outside he sees a non-scalable fence. It surrounds him and encircles both the Ellipse and Lafayette Square as well. He pouts again, pleased. At least until he remembers Georgia, Nevada, Pennsylvania, and Michigan. At Wisconsin, he wrinkles his nose. "How dare they?" After a moment, he smirks. Protesters brave the brisk Autumn air chanting against their own right to suffrage–and all because of him. "Stop the count!" they chant. Others contest "every vote counts" or "count those votes," but they only chant this in spaces where he has been pulling ahead. His oppositionists proceeded to the counters rather than to the streets. "Still," he thinks to himself, "How powerful am I that I have made this many people forget that their former countrymen have died for the civil rights that they themselves now dilute?" His power outweighs his youth, just as his wealth outweighs his power. "Tomorrow will be a day of litigation," he announces to himself, cursing the mail-ins. Yet, the elephant in the room is not the blue counties and states, slipping between swollen rage red fingers. It is the elderly man himself in the center of an oval circus ring once mistaken for a prestigious office.

Washington D.C.

2020

One can only muse what runs through a fading president's mind as they expire out of office. However fictitious these imaginings are, the 2020 U.S. election highlighted just how acute the crisis of electoral systems has become. After the election, heavily

contested vote counts met accusations of corruption on both sides. Suspicious, U.S. citizens' distrust in the electoral institutions piqued. So much that, rounding the final corner of the counts, competing protests rallied behind the mutually exclusive claim of "Stop the Count" and "Every Vote Counts," depending on whether they perceived results were sliding in or out of their favor (LeBlanc, 2021; Earle, 2021). Few moments in electoral history have displayed such distrust in the system that the masses flip-flopped on whether to proceed with it. Although the anecdote references civil unrest generated by former-president Trump before his loss if the 2020 election, similar suspicions were launched by the Democratic party in the 2016 elections lost by Hilary Clinton. Many cited data vulnerability as a contributor (Alvarez et al., 2009). Following a significant information breach in the contentious 2016 U.S. elections, observers noted:

> "No one regulator is responsible for requiring campaigns, political operations and state and local agencies to protect the sanctity of the voter rolls, voters' personal data, donors' financial information or even the election outcomes themselves. And as the Democrats saw in Philadelphia this past week, the result can be chaos" (Bennett and Bender, 2016).

Are voting institutions and their data management systems so vulnerable that being skeptical of vote outcomes may be somewhat justified? If neither side can rest in peace, we need to look beyond the politicians to the institutions they compete within and the technological infrastructure they depend on. Regarding the intensifying challenges in American elections, Norris et al. (2018) suggest we look to theories of motivated reasoning that may elucidate the downward spiral of electoral integrity and descent into hyperpolarization. According to this cognitive science and psychology theory, "new information reinforces opinions, allowing us to make reasoned

arguments supporting our preexisting beliefs rather than changing minds" (Norris et al., 2018; Kunda, 1990; Edelson et al., 2017).

As awareness of vulnerabilities is discovered, the average individual becomes more passionate about their position(s) rather than objective or diplomatic. The protracted crisis of electoral institutions has muddled what was once a relatively cohesive collective belief in electoral outcomes. Some scholars note the ironic negative externalities that certain democratic institutions have suffered due to the democratization of information sharing. For example, in the article, "Can Democracy Survive the Internet?" penned after the contentious 2016 U.S. Elections, Persily notes the complications of formal digital campaigns, the complexity presented by 'fake news' platforms that weave in varying proportions of actual news to gain legitimacy, and the propagandizing role of social media bots (Persily, 2017). At best, the result is social confusion. At worst, we see deepening polarization (as described by Norris' theories of reasoning) and widespread suspicion.

This disbelief translates to genuine concerns for the legitimacy of electoral institutions (Alvarez et al., 2009; Alvarez et al., 2020). In her book, "Electoral Integrity in America," Norris identifies aspects contributing to the declines in perceived legitimacy in electoral institutions and democracy, including "fraud, fakery, meddling and information warfare," among other elements (Norris et al., 2018). Messy as they are, elections can be segmented for analytical purposes. For example, one electoral security report identified three broad electoral phases (the pre-voting, voting, and post-voting period) to organize strategies for fortifying each stage of the cycle (see figure 1).

Designed for conflict prevention policymakers and practitioners, they conducted electoral security assessments in a set of election cases: Guatemala,

Afghanistan, the Philippines, and Burundi (USAID, 7). Alongside comparative insights, the report contributed to the development of the Electoral Security Framework (ESF), a conceptual paradigm geared toward governance programming. Essentially, this framework isolates each component of the electoral cycle and crafts tailored solutions fortifying each part so that the entirety of the system is more secure. The cornerstones of ESF as a conceptual framework are transparency and verifiability. Together, this helps create an audit trail, thus reinforcing the legitimacy of outcomes.

Is this diagnosis sufficiently substantiated? Some question whether triaging tabulation ahead of other corruption concerns is wise. This manuscript does not imply that corruption in other theatres of the election cycle should be ignored but exposes that the latter phases involve a technical dimension that the other sections do not. In that, the final phase is subject to critical concerns distinct from the remaining stages of the election cycle. We'll zoom into the latter ESF phases throughout this manuscript, mainly the voting period (segments 6 and 7), with some analytical attention toward the post-voting period (segment 8). (Please note the following figure from USAID, 2013).

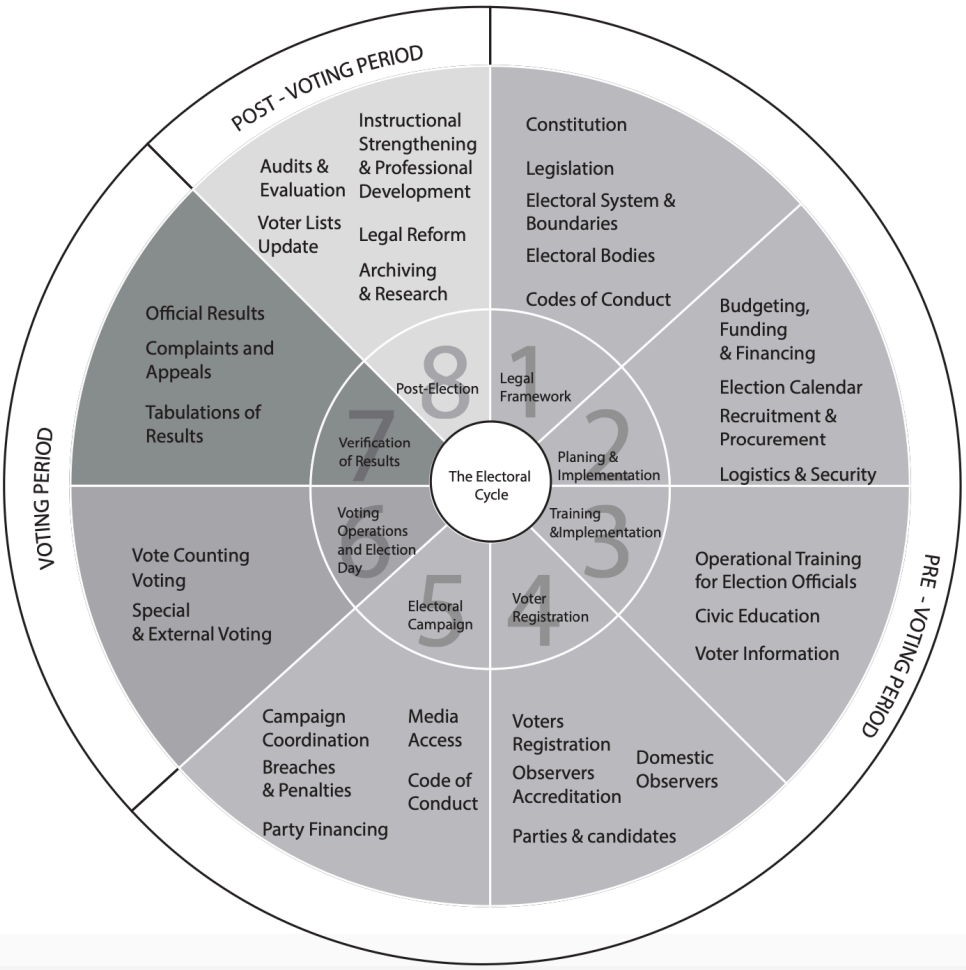

Figure 1. Electoral cycle approach
Source: [USAID, 2013]

In the years since ESF was developed, an increasing interest in data-driven election monitoring has yielded conceptual frameworks oriented toward the security of the digital infrastructure. In 2021, the Cybersecurity Resource Center (CSRC), in collaboration with the National Information Technology Laboratory, developed the Cybersecurity Framework (CSF) Election Infrastructure Profile in response to Executive Order (EO) 13636 issued in 2013 (Brady et al., 2021). The CSF outlines risk mitigation strategies, internal audit techniques and indicates standards for voting system architecture (Brady et al., 2021). Because its scope encompasses voter registration, voting, and voting systems, this conceptual framework is most relevant to the following technical analysis (Chapter 5), risk assessment (Chapter 6), and

policy development paradigms (Chapter 7). As in the broader electoral security concepts offered by ESF, the CSF Electoral Infrastructure Profile also emphasizes transparency as critical to the success of electoral infrastructure (USAID, 2013; Brady et al., 2021). However, CSF zooms into the latter two phases of ESF (the voting period and post-voting period) while acknowledging the evolving and expanding role of technology in registration, voting, and tabulation. The best practices indicated in the CSF Election Infrastructure Profile create a common 'security target' for emerging alternative voting infrastructural approaches and methods, such as blockchain-based systems with lofty promises of transparency, anonymity, and immutability (Zhang et al., 2018).

Whether blockchain alternatives are adopted, in decades to come, 'waiting on Nevada' may be seen alongside the other list of antiquities such as routinely sending letters or stashing one's savings in a sock beneath a mattress and "vest-pocket" ballots of the contentious Civil War era (Rotondi 2020). Essentially, the way we communicate, protect our assets, and elect our representatives have changed—and they will change again. Particularly for the latter (voting), the vulnerability to corruption within today's electoral systems has made this institution so porous that it is indeed a national security risk. Enough cracks exist in the system that warrant a pause for analysis and reflection. According to Time Magazine's Elizabeth King,

> "Voting technology has essentially remained at a standstill for decades. Still, some things have stayed the same even longer: the same concerns for security and secrecy that have kept paper dominant were also the driving forces behind voting policy in the early years of the United States" (King, 2016).

While some argue that simplicity is its best defense, others claim that the current

system is simply stagnant (Abdollah, 2019; Kassem, 2019; Ansper et al., 2010; Crosby et al., 2016; Epstein, 2021). Moreover, recent advancements in electoral technology have *not* kept pace with increasingly complex corruption schemas emanating from political parties (all) and powerful lobbies, colossal private corporations, tech giants, and curious foreign governments—each with a vested interest in the outcome. It is little wonder voters have lost faith in the electoral system within all this jostling.

The fictional anecdote introducing this project hyperbolized the U.S. 2020 elections, but this is an isolated frame for two reasons. First, electoral issues of the technical nature we'll be discussing (tabulation) are *not* unique to the United States but to any country whose elections rely heavily on outdated, easily manipulated Electronic Voting Machine (EVM) technology. Second, major systemic fractures that have been wreaking havoc on today's system began *before* these candidates came of political age. (Let's not give either too much individual credit to politicians for stealing the show when the institution was rigged for drama).

That the U.S. is among the largest democracies in the world (after India) is a contributing factor to significant political gravity (Freedom House, 2018). Statically, however, it is *not* the objective "best" concerning 60 indicators grouped into five categories used to score democratic indices: “(1) electoral processes and pluralism, (2) functioning of government, (3) political participation, (4) political culture and (5) civil liberties” (Bardhan, 2021; EUI, 2021). The EUI defines “full democracy” as any country with an overall score between 8.00 and 10.00, “flawed democracy” between 6.0 and 8.00, “hybrid regime” between 4.0 and 6.0, and varying degrees of Authoritarianism between 0.0 and 4.0 (EUI, 2021).

According to the Economist's Intelligence Unit statistics, the top five ranking democracies were Norway, New Zealand, Finland, Sweden, and Iceland (EIU, 2021).

They boasted respective democracy index scores of 9.75, 9.37, 9.27, 9.26, and 9.18. Among the case studies investigated in this manuscript (Estonia, Russia, Switzerland, Japan, and the United States), only Switzerland (8.9) and Japan (8.15) qualified as full democracies (EUI, 2021). Two case studies, Estonia (7.84) and the United States (7.85), ranked as flawed democracies and only Russia (3.24) ranked as authoritarian.

Following the 2016 U.S. presidential elections, one Vanderbilt research team speculates on the slide from a 'full' democracy to 'flawed' democracy across multiple global indices: "the main reason for the U.S. downgrade to the category of flawed democracy" is attributable to "a drop in the levels of trust in political parties, elected representatives and governmental institutions" (Azpuru and Hall, 2017). This statement is not an 'attack' on the U.S. nor its democracy-loving citizens. On the contrary, it benefits most American citizens to recognize there's a leak in the political plumbing and a few holes in the electoral roof before the entire house floods — again.

Some speculate that Trump's rejection of the loss and the capitol hill storming may have piqued interest amongst authoritarian world leaders (Cliffe, 2021). As Prime Minister Viktor Orbán (Hungary), the hard-right President Jair Bolsonar (Brazil), and Recep Tayyip Erdoğan (Turkey) face contentious elections, might they take inspiration from Trump? In an article titled, "How Strongmen Cling to Power: Authoritarian leaders around the world are strengthening their rule. Can anyone topple them?" columnist Jeremy Cliffe notes:

> "Orbán, Bolsonaro and Erdoğan have systematically attacked their countries' democratic institutions. It is far from certain that legitimate votes against any of them would actually translate into peaceful and just transitions of power…Internationally, democracy has been in retreat in recent years. The global average of the Economist Intelligence Unit's democracy index, which measures the quality of democracy in countries, has been falling since 2015,

> and in 2020 reached its lowest ever level. Hungary, Brazil and Turkey have recorded especially precipitous falls" (Cliffe, 2021).

Though it is uncertain how future elections will unfold, growing trends to reject election outcomes heighten the need for institutional fortification. Is this becoming an unhealthy pattern worldwide? Moreover, to accuse an election has been *stolen* is among the most inflammatory assaults that can be launched in the political realm. However, it's not always clear 'what' has been stolen or 'who' has stolen it. One can argue that an outcome has been stolen (meaning that it should have gone to the rival candidate), but this almost implies that the winning candidate had the perceived capacity to steal it. Although the flaws of the American electoral system do not necessarily amount to outright presidential fraud, legitimacy concerns are particularly acute in the voting and tabulation phases (Norris et al., 2018). Thus, the actual result of rejected outcomes is an incremental theft of trust.

This is perhaps more collaterally damaging to liberal democratic institutionalism than any other factor (Polachek, 1980). Perception is powerful, particularly in an environment saturated with the rhetoric of cooperation, democracy, and cosmopolitanism (Nye and Keohane, 1989). The Electoral Integrity Project (EIP) and Perception of Electoral Integrity (PEI) contextualize the implications of election legitimacy in question on a globally comparative scale via a database called *PEI-7.0* (Norris and Grömping, 2019). Likewise, the Pew Research Center, Heritage Center, the American Press Institute, and Election SOS also track trust perceptions. If an institution fails to meet (or adapt fast enough) to the needs of those that live within it, trust in these structures decreases, weakening it. As this happens, opportunistic political actors can wield a greater role than they would have otherwise. This may explain, at least in part, the rapid rise of populist leaders in countries worldwide.

Legal loopholes contribute to these negative externalities as well:

> "… all electoral system 'manipulate' contests to some degree, such as by the rules used when translating votes into seats. Moreover, procedures undermining free and fair contests can also be perfectly legal, such as the 2012 Hungarian electoral reforms, which favored Orbán's Fidetz government (OSCE, 2014); Malaysia's and Singapore's ethnic gerrymandering, which maintains the power of the ruling parties (Fetzer, 2008); U.S. state laws disenfranchising felons and prison inmates (McGinnis, 2018); and Turkey's high vote threshold, designed to exclude Kurdish nationalists." (Norris et al., 2018: 13).

In our everyday lives, we can feel trust or its absence, but— because everyone has their own interpretation of what "trust" is — the best we can do is quantify the perception of trust. One Pew Research survey studying trust trends amongst 10,618 Americans showed that reported levels of trust were down relative to recent reports and long-range surveys alike. For example, in 1958, over three-quarters of citizens "trusted the federal government to do the right thing almost always or most of the time." Yet, by 2021, only 36% of left-leaning and just 9% of right-leaning affiliates reported that they agreed with this statement (Rainie et al., 2022).

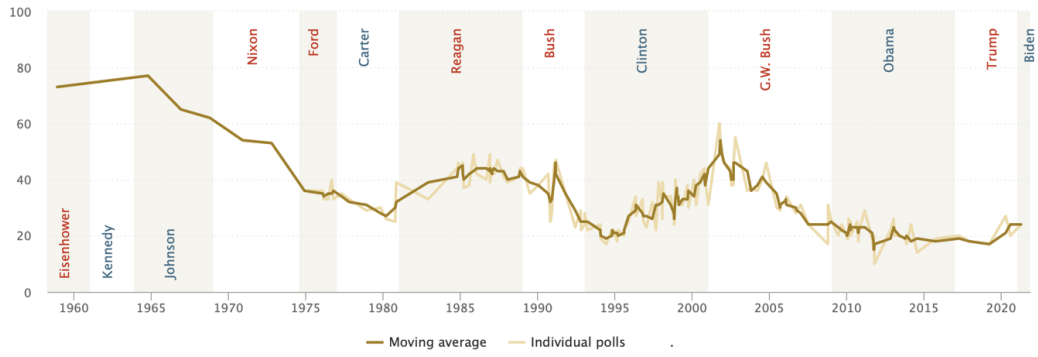

Figure 2. U.S. public trust in government 1958-2021
Source: [Pew Research Center, 2021]

Concerning elections, 53% of participants trust that their fellow citizens will accept election results. In comparison, 47% do not have much confidence their peers will swallow the verdict (Rainie et al., 2019). Trust is not only declining in the federal government but between each other. So, how much (or little) is needed to maintain a stable bureaucracy? (*Please note that I did not say 'democracy').

> "On a grand scale of national issues, trust-related issues are not near the top of the list of Americans' concerns. But people link distrust to the major problems they see, such as concerns about ethics in government and the role of lobbyists and special interests" (Rainie et al., 2019).

There is, however, a silver lining to this situation. The growing lack of trust in the federal government is perhaps the only item both parties of this highly polarized system agree on. The same survey found that 84% of Americans felt trust in the federal government could be improved, and 86% felt it could be restored amongst each other (Rainie et al., 2019). This means that a substantial and objective initiative aimed at fortifying federal institutions would likely receive support and funding from both sides. In other words, if a serious suggestion were presented to entities with the means to back it, political polarization would be less likely to shoot it down before take-off than competitor party-affiliated initiatives.

Thus, trust— rather, the perception of it— represents a collective belief. Peter Racsko, a scholar from the Department of Information Systems at the Corvinus University of Hungary, makes a powerful observation about blockchain's potential influence on collective memory (Rackso, 2019*).* Because every operational aspect of the chain depends upon consensus protocols (see chapter 4) and leger data immutability, this could function as a public transcript (Rackso, 2019. However,

though this is a novel way to reorient our perception of the technology in a political context, there are some technical over-simplifications with the remaining work. For example, Rackso does not strongly delineate the implications of non-public chains (private, consortium, or hybrid) on ledger administration, ignores the political and corporate dimensions of technological development, and interchangeably uses the terms “Bitcoin” and “blockchain.” (Bitcoin is a *type* of blockchain; they are not the same). That these are not mentioned may lead to an over-confident, rather than cautious, verdict on the merits and risks of blockchain voting (Zhang et al., 2018; Park et al., 2021). Nonetheless, an immutable data record generated by a public blockchain could, hypothetically, facilitate collective memory clarity. Moreover, pairing Rackso’s notion of the blockchain as a tool to strengthen common understanding (via the public, unchangeable ledger) *with* the CSF Election Infrastructure Profile would elevate both conceptual frameworks. If blockchain were to be incorporated into the voting and post-voting phases (perhaps in parallel to the existing system as a double verification), this could organically improve collective belief in institutions over time.

Beyond trust issues and security concerns, there are sincere and severe humanitarian reasons why systemic electoral tabulation problems should be addressed. Significant humanitarian externalities stem from electoral corruption at all phases (Stoddard et al., 1995). In some cases, elections and social conflict go hand in hand. Elections are so contested that, in many regions, there is an itemized ‘election mortality rate’ that identifies the deaths and casualties attributable to recent elections (CCAPS, 2013). That institutions are so lacking that a verifiable number exists to document the danger of elections is as alarming as it is tragic. Though such deaths are preventable, election disputes have catalyzed some of the most violent internal

conflicts of the modern era. For a prominent example of this, one might look at the ongoing humanitarian crisis in Myanmar. Although the groundwork of instability was laid by ethnic strife (to the point of genocide) and extreme inequality, the November 2020 elections—the second democratically held elections since the end of martial law in 2011—shattered this fragile achievement (UN News, 2021). The November election results displayed overwhelming support for Aung San Suu Ki's National League for Democracy (NLD) party. Though she won the 2021 Nobel Peace Prize for her democratic activism despite years under house arrest, many (domestically and internationally) criticized her extended silence on the plight of the Rohingya Muslims (BBC, 2018). When she won by a landslide (82%), both the military and several political parties decried fraud. These complaints were voiced via the post-electoral litigation process through the Myanmar Supreme Court. The military countered it wanted to re-do the elections. When this was denied, they staged a coup d'état on the 1st of February 2021. Major leaders (including both the president and Ms. Suu Ki were detained) and thousands were arrested amid violent protests.

Elections have also dovetailed with social conflict in Africa. For example, studies conducted in Kenya, Nigeria, and several other African nations have found that "elections increase conflict in two distinct contexts: during times of civil war, and in authoritarian systems" (CCAPS, 2013). Other sources also analyzing elections in Africa suggest that "weakly institutionalized settings" play a significant role in the mortality rates associated with attempting democratic elections (Salehyan et al., 2014). In each of these examples, we see different levels of tumultuousness and unrest, but it all stems from a burrowing distrust that what was voted for was not accurately represented. Thus, the frequency of this belief the world over demands

attention (Stoddard et al., 1995; Norris et al., 2018). The vast extent of electoral corruption, external intervention, votes 'cast' by dead persons, and other forms of ballot manipulation illustrate two critical points to the thesis of this project:

i. Elections do matter–so much so that individuals will go to great legal and illegal lengths to affect the outcome.
ii. Those pursuing illegal means have been able to do so with greater anonymity and scope because of technological capacities outpacing bureaucratic adaptation.

The only way trust can be rebuilt is to reduce vulnerability to corruption, manipulation, and system hacks. Clean-up is far easier said than done. The straightforward aim of this project is to take a creative stab at it. Throughout this project, we address "electoral corruption" as a larger institutional dilemma, not as a "he-said-she-said" showdown of any given electoral debacle. As such, all examples and cases presented are nonpartisan. At no point will any political party, party member, or affiliate be praised or attacked. The root of this project is, in fact, humanitarian. Better electoral verification practices lead to greater trust, lower levels of civil unrest, and, consequently, lower mortality rates (Salehyan, 2014). Thus, this in-depth analysis aims to investigate not how to bolster trust (through rebranding, media manipulation, foreign intervention, and algorithmic games) but to bolster *the reason* for trust in the first place: election accountability. On the tailwinds of the two assumptions mentioned above, this study targets two analytic aims:

i. To validate efforts to build sustainable institutions instead of propping up the fickle political actors within them

ii. To present an actionable alternative for reducing electoral corruption

Another supportive objective of this manuscript is to iterate the importance of due diligence before implementing any of the alternative e-voting mechanisms presented; asymmetries in quality are already apparent emergent cases thus far. Another goal is to bridge the gap between politicians (clients) and technicians (designers). The former needs an awareness of the political, legal, ethical, and power balance issues that may result from either misappropriating this technology (or premature implementation). The latter need to be cognizant that technological advancement comes with (sometimes irreversible) socio-political costs.

This also work hopes to deconstruct a few incorrect yet colloquial biases that could harm our societal and individual relationship(s) with this technology. For example, when we discuss "blockchain," we are not using the term as synonymous with crypto and other fin-tech derivatives. That mistake happens when one *equates* blockchain with cryptocurrency. The latter exists courtesy of the former; they are not the same. Nonetheless, this confusion has an interesting origin that may explain a more profound social misconception. Encrypted currency (crypto-currency) was yet another push toward a data-centric society. Digital banking presented us with a way to send and receive numeric quantities representing bills we never saw, whose physical presence mattered less than its believed existence.

Cryptocurrency differs because it solidifies—in the financial world— a new abstract phenomenon. In the crypto world, value has been re-conceptualized, not just for its numeric significance but as data. This understanding underscores an even larger dynamic. Data carries a greater inherent value than currency. Data can take the form of money (in the form of a currency, coin, or token) but not all money can "be"

data. Thinking in ‘financial’ terms is limiting. Doing so constrains our focus on the concept that what is transacted has a typical ‘monetary’ value when it’s more than that.

This analysis is more interested in the way data is transacted (per this analysis, a vote) and what can be done to protect that personal data. Again, the crux of this blockchain use-case analysis is security— not finance. When we break that down further, this project has taken a policy path (macro-analytics) rather than engineering (micro-analytic). Likewise, all technical explanations provided inform the context of these policy paradigms about alternative blockchain e-voting systems, while all theories orient our social relationship with this new infrastructure. Though all of the projects mentioned utilized open-source code, none of the coding or algorithmic components have been included— we only discuss theoretical aspects of how they fit together. Lastly, the perspectives discussed throughout this manuscript descend from a fusion of managerial cybersecurity paradigms, political theory, and philosophy more than finance or economics.

It is already impossible to control for all external variables affecting election security (money, social media, political parties, advertising, back-room deals, siloing of mainstream media, gerrymandering to non-competitive districts, foreign interference, etc.). On top of this, we must also consider general inaccuracy and human error. In short, the current systems, which have worked for centuries, are losing credibility from some, if not all, of the reasons mentioned above. Thus, the aim of this analysis is to reduce vulnerability to corruption, manipulation, and error in the counting process. That there is a perception of fraud at all steps in the current election process (exacerbated by theories of reasoning and polarization) is, in some ways, more important than whether it exists (Rainie et al., 2019). Perception is

reality. That society craves a resolution is evidenced by sporadic pilot-testing of alternative voting systems worldwide, such as blockchain e-voting.

Since a complete reversal to traditional paper ballots is improbable, tomorrow's alternative systems may rest the vulnerabilities of today's e-voting machines (EVMs) (Gonzáles et al., 2020). In spaces where blockchain-based e-voting alternatives have been implemented, have these alternative methods been outpacing conventional techniques? Or have they introduced new challenges with risks outweighing opportunities (Park et al., 2021)? The following outlines the problems embedded in conventional voting systems and addresses the prospects of moving forward given the knowledge gained from five case studies: Estonia, Russia, Switzerland, Japan, and the United States. Each case highlights a unique way in which a blockchain enables an alternate data management system where voters can cast their ballots.

Thus, this investigation does not look outward — in an attempt to thwart corruption, manipulation, and human error— but inward at the data management systems and voting infrastructure for a less vulnerable alternative according to modern security standards outlined by the Cybersecurity Framework (CSF) Election Infrastructure Profile. However, whether the answer lies in blockchain, this investigation ultimately touches on our understanding of the political relationships between the individual, society, and the technological architecture we've constructed to organize our bureaucracies.

Implementing blockchain-based e-voting systems would invite an entirely new way of organizing the data of all citizens within a nation; at scale, this could reorient how we organize society and ourselves within it. Ultimately, policies on blockchain e-voting must solve how to best fortify electoral systems and protect the

users they intend to serve without introducing greater risk. Although this thesis is designed for academic purposes, the policy paradigms, analysis, and concerns presented here are also relevant to the fields of cybersecurity, information system security, network administration, and system architecture.

CHAPTER 2

THE EVOLUTION OF VOTING TECHNOLOGY

In the computing world, “system patching” refers to any prescription of changes made to a program or supporting features to update, improve, or fix problem spots. This targeted mentality underpins the methodological backbone of this research. After an initial overview of issue areas, this analysis seeks to identify ways to patch them up. We’ve already taken a few detours into how voting machines have been exposed to manipulation until 2015 (Epstein, 2020; Schneier, 2004). We also delineated ‘the theft of trust’ as a threat to electoral institutions and, by extension, security, and sovereignty (Orr, 2016). Will it all come crashing down next campaign season? No. Will an increasing number of individuals question the legitimacy of the outcomes? Very likely. Though it’s sexier to market political Armageddon, the gradual erosion of trust in electoral institutional legitimacy is a more sinister culprit (Salehyan et al., 2014). As with any discussion of institutional improvement, tracing how this institution evolved (or unraveled) over time is symbiotic to understanding the technical features that must be addressed today.

Four metrics can help us articulate and measure 'optimization' from a systemic angle: accuracy, anonymity, scalability, and speed (Schneier, 2004). If the goal of electoral technology is to improve these metrics holistically, how does our current system measure? True, we've come a long way since stones and ceramic potshards were dropped into ancient Greek vases (Kosmin, 2015). Since paper ballots and voting boxes came onto the scene, there have been remarkable developments (King, 2016). Mechanical voting booths, punch cards, and optical-scan machines replacing the manual work of hand-counted ballots sparked unprecedented

acceleration (King, 2020). Yet, the evolution of voting technology is an ironic one, where each 'upgrade' has impacted these basic tenants with an asymmetric hand (Schneier, 2004). Dramatic gains in speed and scalability have sacrificed accuracy and, at times, anonymity in the process.

Doing due diligence on each of these metrics is not just a matter of technological capacity but security. Accuracy becomes impossible if an individual's vote is changed, destroyed, or affected after its cast. Stuffing ballot boxes (among other fraudulent activities) incur equal damage (Norris, 2020; Alvarez et al., 2009). Likewise, a lack of anonymity (i.e., "the secret ballot") jeopardizes voters, voting rates, and the strengths of the democratic systems they are situated within (Asenbaum, 2018). Suddenly, the immense achievements in the speed and scale of such systems create an ever-greater cause for concern. Not only are errors occurring right and left (no pun intended), but these errors carry a booming echo.

Moreover, ballot tabulation errors are not uniformly distributed. These sporadic distribution mistakes make finding the source of such problems that much more complicated. Not factoring in the discrepancies caused by external hacking, computerized system errors (associated with the individual machine), and software system errors (systemic issues related to the entire program) negatively impact electoral efficacy.

It’s no accident that this manuscript began with a political photograph depicting a circus. Though it is incredibly descriptive of an integral moment in the larger global political arc trending towards volatility, determining what normative policy line we should follow to calm it down demands greater analytical legwork. Using clues from this snapshot to identify and analyze potential factors contributing to this problem allows us to target the root causes rather than symptoms of this multi-

level chaos. In this case, the symptoms culminate in social conflict, institutional trust issues, contested results, declining perceptions of legitimacy, greater susceptibility to hacking and foreign intervention, and, above all, heightened national security risks.

Peeling away the issue, the outermost problem we encounter is electoral tabulation. True, it's not the only problem with elections. We could always go deeper, noting the questionable influence of private donors and lobbies, shady partnerships, bridges, scandals, insider information leaks, and the other controversies that litter the campaign trail en route to the polling booths. However, if we cannot manage the instrumental aspects of elections, what good would these efforts be? All phases are worthy of being addressed, but (for now) this research aims to reduce vote tabulation errors. This means systemic assessment and (potentially) policy revision. It benefits no one to rely exclusively on hawk-eyed audits; instead, we should aim to prevent problems before they start.

Throughout this analysis, we hope to contribute to the broader dialogue of theories and relevant literature on institutional integrity, election security, cybersecurity paradigms, and blockchain initiatives (including emerging e-voting techniques). The central hypothesis guiding this research is that a blockchain-based system can improve the accuracy, anonymity, scale, and speed of the vote tabulation process. An equally important objective is to mitigate existing risks without introducing new existential threats to voting security. Such a change would be a revolutionary improvement over other lurching techniques— that have typically increased the speed and scale at the expense of accuracy and anonymity (or vice versa).

In the following sections, we'll discuss both the technical and abstract dimensions of the analysis (such as the ethical, legal, political, sociological, economic, and financial elements) and the risks of implementing such technology too soon or too late. Following a thorough theoretical investigation--- system patching the tabulation hardware and software from start to finish— it's likely that one of the most significant barriers to building a tangible beta model will be funding. We find that whether blockchain alternatives are appropriate, there is a dire need for safer, more efficient hardware and software inputs. After, we'll review the literature on relevant use-cases where scaled chains have been put to the test around the world.

2.1 Categorizing tabulation technology

Hassan et al. define three main technological categories for vote tabulation technology: (1) traditional (paper-ballot), (2) electronic (e-voting), and (3) alternative e-voting systems (most notably, blockchain-based) (Hassan et al., 2022). Traditional tabulation technology relies on classic paper-based ballot submissions. It typically demands voters and polling agents to be present at designated polling stations. Basic operating costs include paper, ballots, EVM machines, and employee salaries. Though forgery, counting issues, and security dilemmas are not infrequent. Likewise, procedural delays translate to lagging outcome announcements as well.

In contrast, electronic (e-voting) systems depend on entirely electronic voting machines (EVMs) and a fully centralized system. The data is vulnerable to mutability (I.e., votes cast can be illegally destroyed, duplicated, or revised) despite claims otherwise. This is because EVMs need an internet connection and web connectivity to work. Although there is more transparency than with paper ballots, the weight of political influence shifts in favor of a tight oligarchy of EVM producers. The highest costs are upfront: producing, certifying, and setting up the machines with tabulation

programs.

Some of the earliest EVMs were developed in India (1989) by the Election Commission of India with Baharat Electronics Limited and Electronics Corporation of India Limited / ITT Bombay. However, the EVM development journey began over 100 years earlier, starting with late-Victorian mechanized prototypes. In 1848, Francis H. Smith, Stephen Bowerman, and R. E. Monaghan invented a mechanical voting mechanism. When the Committee on Public Buildings and Grounds declared modernizing the system was not necessary, the proposal fell to the wayside until Thomas Edison emerged on the scene in 1869. With his freshly-patented telegraphic voting machine, he presented his invention to the House committee—who also shot it down. Their primary reason was that it would slide legislation through so quickly that procedural minority rights might be at greater risk of being side-lined. It took another nearly twenty-year leap (1886) before it was brought back into the limelight by Lewis Beach, a representative from New York. He became the first to introduce a formal resolution to peer "into the feasibility of a plan for registering votes." Politicians thought about it for 30 years before the Committee on Accounts initiated a hearing in 1916 (H. Res 223). These were the conditions at the time:

> "A clerk would read out the name of each Representative, who would respond to their names by calling out yea, nay, or present. By the time the House reached its current size of 435 Representatives in the 63rd Congress (1913–1915), *each* recorded vote took around 30 minutes— sometimes longer" (U.S. House of Representatives: History, Art, and Archives, 2022).

The hearing resulted in a new commission investigating prospects for an automated voting system. This step forward was allowed following assertions from an electrical engineer wielding a delectable incentive: a mechanized solution could save them 50

legislative days annually. Though it received more significant support than previous pitches presented by innovators to politicians, the resolution was shot down. In January of 1969— a full 121 years after the initial mechanized prototypes were introduced—the House Democratic Caucus allowed an internal resolution (not a binding document, but one representing prevailing sentiment) to request that the Clerk begin considering improvements to voting procedures. This issue was passed to John McCormack, the Speaker of Massachusetts. McCormack then directed a man from Maryland, Samuel Friedel (Chairman of the Committee on House Administration), to scout out opportunities.

By April, the Clerk (William Pat Jennings) released a report detailing system requirements. Alongside user-friendliness, it was essential that the new voting system "conform to the design of the historic House Chamber" and follow the most straightforward design possible (U.S. House of Representatives: History, Art, and Archives, 2022). In addition, the Clerk emphasized transparency: a display board would show the title and number of the bill being voted on and the Member names of those voting plus a running total of all votes. Lastly, this system would need to accommodate inputs from various polling stations scattered throughout the chamber and maintain correct counts.

In the transition phase before adopting EVM technology, a representative from Michigan (Lucien Nedzi) visited Sweden to view their implantation of the electronic voting technology. Upon his return, Nedzi's report and findings became the impetus for the "Legislative Reorganization Act" of 1970" which officially allocated funding for developing an EVM system. However, it wasn't until 1973 that it was put into practice in the House via a 15-minute roll call. From that point onward, only minor changes were made, such as exchanging analog vote cards with

computer chips (1999-19970 and creating braille-equipped stations (2018) and DRE-styled touch screens used today.

Though it's taken significant insistence, revision, and compromise, it's already been made clear that today's EVMs are far from their evolutionary peak. Another contributing factor to these issues is the vertical manufacturing production process of EVM machines. Fallible system presets and low-standard approval thresholds are just the beginning of their problems. Simply put, an oligarchy of private producers was tasked with making a "box that counts." These producers, who specialize in producing, not cybersecurity, built a box that counts. We should not be surprised that these boxes are vulnerable to tampering. Likewise, acknowledging the lack of discretion in preset access codes, it may also be wise to reconsider the present outsourcing of manufacturing components in favor of domestic production. This becomes particularly important when we acknowledge that manufacturing presets might be confidential beyond the manufacturers/producers and administrators. Still, if confidentiality is <u>not</u> limited internally (amongst the manufacturers and producers), it is compromised. This is a significant breach, more so when one also traces aspects of the foreign supply chain back to dubious origins.

More alarming, determining which hardware will (or won't) be selected is, often, neither proper security nor functionality question but a business one. Even if, by this point, employing blockchain technology to optimize today's electoral systems seems far off, it's worth optimizing the incongruence in the existing manufacturing chain. Who owns America's voting machines? France? The U.K.? Others? Are they public property (government-owned) or run via private enterprise? Is this country dependent, or is this pattern repeated across the globe? Over half of all countries mandate voter registration (122 out of 226 members of the ACE Knowledge

Network) (ACE Project Data, 2022). Before the 2020 pandemic, about one-fourth of these (40 countries) used postal ballots (Norris et al., 2019). Most of these were in Europe, North America, and Asia-Pacific. However, overwhelmingly, most countries (209) worldwide used paper ballots (ACE, 2022).

Countries that use electronic voting machines (EVMs) must purchase their EVMS from a tight oligarchy of manufacturers. In North America, three private companies run the show: Election Systems & Software (ES&S), Dominion Voting Systems, and Hart InterCivic. They court consumers, namely government representatives wielding large budgets: "…the vendors often spending thousands of dollars to sponsor conferences and receptions attended by the officials. The industry also hires former election officials to represent them" (Fessler and Kaufman, 2019). Further, in the ongoing debate about whether collaboration between election officials and EVM vendors is ethical or compromised, accusations of illicit behavior were disavowed, but open cooperation ceased. Eugene DePasquale inquired 67 county electoral officials to report any gifts or favors they'd received.

> "Eighteen said that they had, with the gifts ranging from expense-paid trips to Las Vegas, to winery tours to boxes of chocolate-covered pretzels…even small gifts, which are allowed under state law, 'smacks of impropriety.' The state expects to spend some $150 million on new voting equipment for next year's elections and competition between vendors to get a slice of the business is fierce. DePasquale says decisions about what equipment to buy should be based on 'security and long-term effectiveness for the voters as opposed to who was taking people out on wine tours and amusement park trips.' He says he has no evidence that the gifts have influenced specific buying decisions but says even the appearance of special treatment undermines public confidence" (Pennsylvania Department of the Auditor General, 2019).

Even the most superficial AVS market analysis tells us that there's room for foul play not only in the manufacturing of these machines but in the selection of business partners before even beginning the manufacturing process. Ultimately, the polling stations needed a box that counts. Businesses met that demand and supplied a box that counts. Though they took some cautions with security, they were not as high a priority as locking down the distribution contract. After the contract was secured, these companies — according to several sources—received shockingly little oversight (Norden et al., 2022).

> "Election officials from across the country buy much of their election infrastructure from private vendors. These companies build and maintain registration databases. They create election websites that explain how to register and where to vote. They manufacture and configure voting machines. Yet unlike vendors in sectors the federal government has designated as "critical infrastructure"—like defense and energy—companies in the election technology space operate under very little federal regulation**.** While voting systems face some functional requirements through voluntary submission to federal testing and certification, vendors themselves are largely free from oversight" (Norden and Beard, 2020).

The dynamic amongst EVM producers does not unfold with the competition prevalent in the tech industry, where there is an unceasing, almost brutal, push to outdo contemporaries. In this realm, there is comfortable nepotism, and the political dynamics that play out are more about paying back favors. Though there is undoubtedly a political dimension and personal-network element to the tech realm, poor performance won't save you. Perhaps the most self-evident indicator of the top-down stagnancy of EVM manufacture is that there is no shortage of skilled persons able to build better machines, which means there is a deficit of manufacturer or upper-level demand. Likewise, there is little security logic to outsourcing

components of EVM manufacturing to foreign nations aside from the status quo.

Alongside the peculiarities embedded in designing and producing the hardware for these machines, other questions remain. For example, what happens to decertified devices? Though some have a more advanced set of diverse functions, these machines are only built for *one* purpose. Are they modified or repurposed for other endeavors? Or modified and recycled back into the system? Who buys them and why?

The EVM life cycle is wormed with security holes--from its certification and manufacture to its decertification, dismantling, and re-sale (Thielman, 2015; Epstein 2015). For example, the National Institute of Standards and Technology (NIST) and the Election Assistance Commission (EAC) co-created a set of technical standards after the presidential elections in 2000 (Bennet et al., 2016). However, because these standards were non-binding and perceived as 'voluntary,' the problems they sought persisted decades later. Moreover, the EAC, which is intended to conduct audits and safety test machines before certification, is largely funded by the dominant EVM producers themselves (Thielman, 2015). The EAC also has a problematic history with leadership: "For three years, the EAC limped on without confirmed commissioners—an EAC commissioner stepped down in 2005, calling its work a 'charade'" (White et al., 2022).

In addition, the private sector produces the primary hardware components used in the EVMs, with questionable overseas links and unchangeable manufacture presets from a limited set of options in a low-diversity in manufacturer-oriented market. The current system is not slated to benefit their customers' security interests but the vendors themselves.

There may be some arguments that where isolated parts of these machines are produced become irrelevant (from a security standpoint) and more cost-effective

(production-wise) if the software is robust. (Software concerns consist of computational components, troubleshooting, bug fixes, manufacture presets, administrator access; their purpose is primarily accuracy and securitization). However, it's clear (as we've seen in that last chapter) that this software has exploitable quirks that make it far from secure. So, while it's necessary to mention the manufacturing system concerns (for the sake of being thorough), this project focuses far more on the technical problems posed by the EVM software in practice.

Regardless, there are a few key differences between traditional tabulation technology and e-voting systems. The first is that EVM-based systems are fully centralized. In contrast, traditional paper-based ballots relied on a physical or locally deployed system. This, paired with mutability, makes the EVM-based e-voting system significantly more vulnerable. Likewise, all e-voting machines depend upon web connectivity meaning data has thinner protection as it journeys on the internet highway. However, the upside is that results are significantly faster, the process is more transparent, and most operating costs are upfront rather than recurring (Hassan et al., 2022).

Alongside how data is collected (hackable networks), there is also the cryptographic concern of how information is encrypted, decrypted, and stored. Cryptography is considered "the art of writing or solving codes" (Oxford Languages, 2022). Encryption is the first part (writing) or converting information content into code. The second part (decryption) happens on the receiving end when the recipient must untangle the code and retranslate it back into the original information content. (Note: this is also the origin of the term 'cryptocurrency,' i.e., encrypted currency). Other issues arise once this vulnerable information (your vote) is sent to the polling stations' central database. (The following 2019 figure is from ATP electronics).

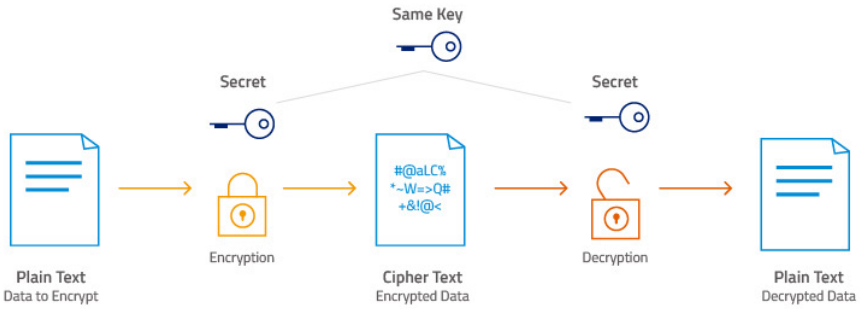

Figure 3. Symmetric encryption
Source: [ATP Electronics, 2019]

Existing EVMs must use cryptography because it is necessary to translate the physical information of your paper vote or mail-in into digital terms. But how is that data stored? The answer stands front and center of the critical arguments dividing Mac and Windows user preferences. We all know that Windows hardware is more flexible for developers and more manageable to upgrade (among other things). Still, it is also known to demand greater vigilance when protecting from malware and third-party viruses than its leading competitor, Mac. Why? In the same vein, surveys reveal that "more Americans trust Microsoft than Apple with their private data, at a rate of 75% to 69%" (Blake, 2020). When both openly admit to selling information to third parties, it seems backward to be more willing to trust the more monolithic, less transparent of the two tech giants. So, why does one desktop operating system have a more substantial reputation in terms of security and privacy than the other? (Again, the perception of *t*rust helps direct us toward the heart of the issue).

One of the possible reasons for this phenomenon overlaps precisely with the security discussions surrounding EVM technology: localized encryption versus hardware encryption. For example, Mac uses a built-in FileVault to encrypt data with a 128 AES encryption and a 256-bit key. AES stands for "Advanced Encryption Standard." It's a U.S. Government-approved symmetric block cipher (using the same

key for encryption as decryption). A “bit” is an abbreviation for “binary digit” with a value of 0 or 1. In the context of security, these bit keys or encryption keys are generated in a random sequence. Among the four champion encryption methods (AES, Rivest-Shamir-Adleman (RSA), Triple DES (Data Encryption Standard), and Twofish, AES is known as the most heavy-duty (ATP Electronics, 2019). In hardware encryption, data is kept separate from the functioning of the computer, contained entirely on the hard disk. However, in local encryption, even if one were to encrypt every file of data they processed, a second (parallel) version of that same data exists in the computer’s temporary memory. These encryption differences contribute to why you can’t run Windows software on a Mac and vice versa. To run any Windows software on a mac, you must either partition the macOS hard drive or use a parallel desktop. That partition is the equivalent of you consenting to use a portion of your computer to encrypt and decrypt data according to the localized process. In other words, whatever content is in the temporary holding space (while being stored locally) is not encrypted and therefore vulnerable to attack.

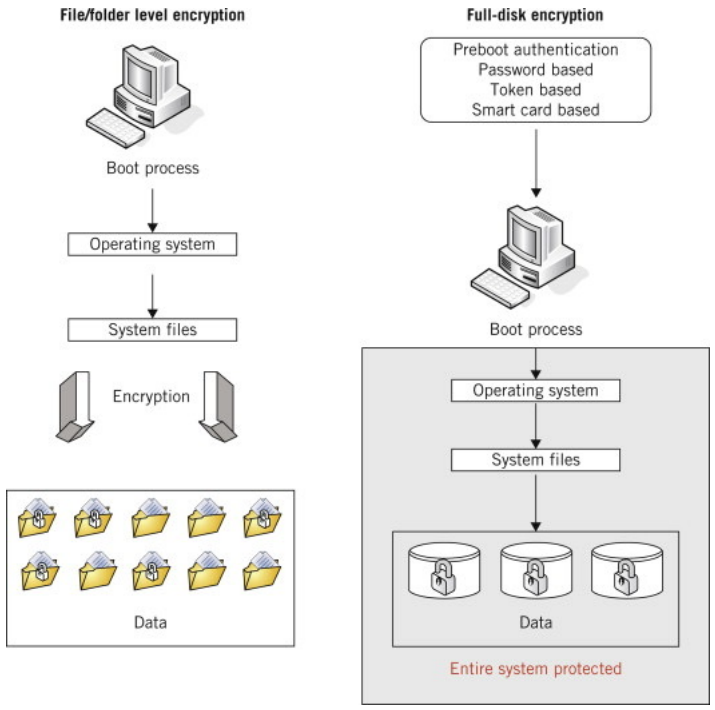

Figure 4. File-based encryption vs. full-disk encryption
Source: [Chuvakin et al., 2010]

The terms "File/folder level encryption" can be used interchangeably with "localized encryption." Likewise, "Full-disk" encryption is equivalent to "hardware encryption." The latter (and safer of the two) segregates data from the operating system *via* its hardware—preventing any potential breaches from contaminating the operating system. So, suppose a virus finds its way into the data. In that case, the hard disk can be restored fully with lower risk. A previously-backed-up version of the data can be re-uploaded to the drive— without impeding the functionality of the operating system or — as often happens in Windows— inadvertently re-introducing the virus following device restoration. Thus, hardware encryption directly encodes data onto the hard drive, meaning that to restore it or wipe it clean of viruses is to address only the hardware of the machine itself—not risking the operating system. This is widely considered the safest encryption type. However, the main producer of operating systems using this encryption method is Apple, a private entity with its

own gravitational economy so large that it casts a shadow over rules and regulations intended to tame it from abusing privacy laws and price gauging. Apple possesses an incredibly tight monopoly over its operating systems— so closed that it would be a risk to use Apple-based products to conduct a national election. Doing so would simply diffuse power over key security components between government entities, and a private entity whose market cap (worth over 3 trillion USD) outperforms the GDP of the entire United Kingdom (Smith, 2022). Though Apple has no military and is bound to the legal headquarters (Cupertino, California), it carries the economic weight of a country. Thus, engaging Apple is to invoke a near-autonomous technocratic entity with no true national loyalty — only a devotion to profit. Where privacy rights and profit compete, profit wins. The question grows equally complex when considering government perspectives: where national security and privacy rights compete, security wins. The San Bernardino Case resulting in a major dispute over encryption between the FBI and Apple illustrates a tense dynamic boiling between tech giants and the government bureaucracy (Nast, 2022).

Following a terrorist attack in San Bernardino, California (2016) that killed 14 people, there was extreme FBI pressure to violate privacy to determine the identity of the perpetrators via an iPhone identified in a security video. However, on the grounds of privacy protection, the U.S. government could not legally impose Apple to reveal the identity of the watch-wearer who committed the crime.

> "Setting up a pitched battle between Silicon Valley and the counter-terrorism community, Apple's chief executive said Wednesday that his company would fight a court order demanding the tech giant's help in the San Bernardino attack investigation, turning what had been a philosophical dispute into a legal skirmish that could have major ramifications for the tech industry" (Lien et al., 2016).

However, within less than 24 hours, an Israeli intelligence organization (based in a lucrative region known for cybersecurity and intelligence operatives known as "Silicon Wadi") hacked the Apple platform and determined the identity with apparent ease. Though the issue of identifying the terrorist was resolved in the short term, no conclusive legal precedent for the future was determined. Layered on top of this, the unspoken east-west divide between the lobby oligarchies encapsulating Washington D.C. (and elsewhere in East Coast metropolitan centers) and the tech bubble (predominantly rooted on the West Coast, most notably in California) worsened. If the "hack" were to have been conducted explicitly through U.S. Entities, it would set an extremely dangerous precedent for privacy laws (Segal, 2017). The politico-legal path of least resistance was to outsource the dilemma. In legislative terms, the ethical dimension posed the greatest barrier. However, in technical terms, there was little actual barrier to the privacy of the individual users. These 'protections' were stripped with ease. Though the user happened to be a terrorist in this circumstance, what happens when the user is a law-abiding voter? Even in the more 'secure' of these encryption options, there is little anonymity— especially if discrepancies are shuffled overseas for resolution. Lack of transparency is dangerous in governance. Is this a system that would be ideal for conducting a national election? Probably not. Relevant to this analysis, there are two takeaways from the San Bernardino case. First, the individual appears to be a pawn that both sides use to justify their actions. Technocrats use the rhetoric of privacy rights to reinforce their own autonomy— while committing violations themselves. The government uses national security — and prospects of collective security— to claim the net result of violating privacy laws creates a holistically safer space. Second, even an entity as isolated as Apple is not impenetrable— legally or technically.

For this reason and others, we're then left with a Windows operating system offering greater transparency and flexibility despite the risks it poses. Despite the flaws of the Windows operating systems used by American EVMs, it appears wiser *not* to engage the private monolith Apple for the purposes of conducting elections. This is not because privacy laws work when put to the test, but because verifying Apple's reports (without flaring the U.S. legal system) would require enlisting an overseas third party (as happened in identifying the terrorist attacker) to compromise— only this time, it would compromise millions of innocents, not one criminal. Until a safe and scalable version of a blockchain-based e-voting system (or some other alternative) is ready, we should triage. This begins by changing EAC regulations to no longer accept outmoded operating systems. All machines must be certified by the EAC; therefore, they should be dictating their preferences to producers, not the other way around. Second, since both voter-verifiable (paper) ballots and unverifiable (electronic) ballots are all ultimately digitized and stored in a central database, then the internet connection of those databases must be airtight. That this has not been happening is both embarrassing and outrageous. Accomplishing these two milestones within the next two years would, at least in part, reduce the hackability of votes cast in the next presidential election.

Moreover, although the bureaucratic approval and certification process should be methodological and thorough, it should not be so slow that it fails to adapt to the present technological needs. It has long passed when that slowness has posed a significant security problem. As reporter Tami Abdullah points out, "the vast majority of 10,000 election jurisdictions nationwide use Windows 7 or an older operating system to create ballots, program voting machines, tally votes, and report counts" (Abdollah, 2019). This is not the only alarming feature of her observation.

She presses onward:

> "… because Windows 7 reaches its "end of life" on Jan. 14, meaning Microsoft stops providing technical support and producing 'patches' to fix software vulnerabilities, which hackers can exploit. In a statement to the AP, Microsoft said Friday it would offer continued Windows 7 security updates for a fee through 2023" (Abdollah, 2019).

Not only is Windows 7 a porous and vulnerable operating system, but that extension is entirely useless given that the next election will be hosted in 2024. This is the most superficial layer of the problem. The immediate course of action is equally surface level: upgrade it to a later version. To understand the deeper origins of the tabulation dilemma (in the U.S. case study, at least), we can't overlook how these elections are accounted for from a politico-infrastructural (rather than technical) standpoint. We'll dive into international experiments with alternative election verification methods soon. However, the U.S. presents an ideal case is not only because it presents an unusual internal state-nation state dynamic but because it's frenemies with one of its largest sources of global soft power: tech giants headquartered inside its own borders who possess so much power that they can (and do) disobey regulations attempting to curb that influence where it conflicts with the national interest.

In the U.S., the majority vote does not choose the president but rather the majority of the 538 electors of the Electoral College (The Straits Times, 2020). The popular vote elects the electors, who then vote on the president and vice president. Every state is divided (and subdivided) into precincts (voter districts) responsible for receiving and counting (ACE Vote Counting at Polling Station Data, 2021). At least 270 electors must vote for a candidate for them to win the presidency. There are several types of electoral voting (First-past-the-post, block-voting, the runoff system, proportional representation, and ranked voting).

There are two main layers to conducting counts: a "central count" and a "precinct tabulation." In a central count, election workers of mixed political parties transfer ballot boxes to a central country location. In contrast, a precinct tabulation stipulates that one must not move the ballot boxes from the polling station (place of voting), nor are vote counters allowed to leave the site until counting is complete. They open, sort, reconcile, and count the ballots on-site— localized (Azclean, 2021). They conduct all counts on a live video feed and other measures, "ensuring the physical security of all ballots. Protecting ballot security includes the use of tamper-evident seals, identification badges, the presence of two or more staff members of opposite political affiliations, audits…" are adhered to. Three machines mitigate human error in the process: (1) an optical scan paper ballot system, (2) a direct recording electronic (DRE) system, and (3) a ballot-marking device and systems (BMDs) (Ballotopedia Data, 2021). However, several states use traditional hand-count methods to verify the mechanized system: Alaska, Colorado, Idaho, Kansas, Maine, Massachusetts, Minnesota, Missouri, Montana, New Hampshire, Texas, Vermont, West Virginia, and Wisconsin (Ballotopedia Data, 2021). While most states use some form of double verification, it is noteworthy that not all states account for their votes in the same way.

Some might argue that these inter-state discrepancies attest to the legacy of subsidiarity. Wherein the states are the basic unit of power. Though this principle was made famous by the European Union, aspects of this philosophy also apply to the United States. Subsidiarity implies that what can fall under local jurisdiction should. Though member states of the European Union interact far differently with the E.U. (a supranational institution that began as an economic alliance) than the states interact with their federal government (a nation-state that began as a collection of

colonies), elements of subsidiarity belly coordinated action in a federation of any kind. Particularly in the U.S. case, when subsidiarity creates significant inconsistency between how votes are counted between states, some argue that may create noise. Worse, it may present logistic confusion regarding standardizing election procedures. That both arguments come from valid observations offers an exciting dimension for analysis. However, net gains appear to be decreasing.

> "Policy on voting is decided by each state and, in some cases, each county—a system illustrated vividly by the trench warfare of voter ID laws that pockmark the country…In total, more than 8,000 jurisdictions of varying size and authority administer the country's elections, almost entirely at the hands of an army of middle-aged volunteers. Some would say such a system cries out for security standards." (White et al., 2022).

Though counting strategies vary according to the state law, a few machines (made by a small oligarchy of producers) became staple electoral technology on a near-unanimous basis. For example, after the electronic voting machine (EVM) and its punchcards debuted in 7 U.S. counties in the 1964 presidential election, it swept throughout the country. Today EVM technology can be seen as a catch-all for techniques from the traditional punchcard method to optical scan systems, voting kiosks, direct-recording electronic voting systems (DRE), and any electronic transmission of ballots via phone, computer, or internet. Though convenient, the DRE is far from foolproof.

2.2 Voting system hacking — and how easy it is

According to several software security sources, one version of the DRE used between 2004 and 2015, called the "Advanced Voting Solutions (AVS) WinVote," was "notoriously insecure." (Its operating system was intended to run until January

12, 2016 (Cortés, 2015). They acknowledged that “insecure configurations, well-known administrator passwords, and lack of patch process” were just the beginning of their security problems. You can think of “system patching” as a review where one seeks to systematically ‘patch’ problems. The patch is a set of changes (revisions) to the computer program or, perhaps, its supporting data. Updates, bug fixes, and improved ‘versions’ are examples of patching security holes. In other words, the AVS WinVote did not have a way of fixing problems even after they were identified.

WinVote was decertified in 2015 and labeled by some experts as “the worst voting machine of all time.” Not only were vulnerabilities identified as early as 2004, but little was done about it (MRSC Data, 2021). Accessing the databases was alarmingly easy. All a hacker had to was target administrator access. Once they did so, they had (read and write) access to all information on the database, including ballot, voting location, and the number of votes. Each database is Microsoft Access, meaning that, though they require a password, none of the databases are encrypted. This is an excerpt from a security report prepared by the Virginia Information Technologies Agency (VITA) presented to the Department of Elections on April 14, 2015, before the system’s decommission.

> “The password on the database provides very limited protection and can be bypassed easily with a hex editor (a specialized tool to edit individual bytes of a file) or identified with a password cracker. A password cracker was used by VITA to attempt to obtain the password protecting the database. The weak password on the database permitted VITA staff to access it in approximately 10 seconds using “AccessPasswordRetrievalLite” to guess the password (“shoup”). This password was used for all of the database files. With the password, it was possible to copy the database files to the security analysis system, open them and modify the voting data. To validate that the changes were permanent and not overwritten by the application’s controls, a hash of

> the file (MD5 checksum) was taken and validated after the database had been copied back to the WINVote device. The hash values matched, confirming that the altered files remained on the system" (Commonwealth Security and Risk Management (VITA, 2015).

Another security report produced by the same agency acknowledged that it was possible to hack the operating system from a parking lot across the street *without* source codes or advanced tools. Using a free sniffer to capture web traffic, the hacker could easily determine the Wired Equivalency Password (WEP), connect to the voting machine via WiFi, access the administrator profile with the password "admin," and download the Microsoft Access database using Windows Explorer. Using the strategy mentioned above (a free tool to extract a hardwired key, "shoup"), the hacker could then access, add, delete, or alter totals in the database before uploading the modified copy back to the voting machine. (Note: These passwords came manufacture-preset and could not be changed after distribution). Jeremy Epstein, an analyst with over 30 years in the field of security who now writes on behalf of Princeton University's Center for Information Technology Policy, notes:

> "If an election was held using the AVS WinVote, and it wasn't hacked, it was only because no one tried. The vulnerabilities were so severe and so trivial to exploit that anyone with even a modicum of training could have succeeded. They didn't need to be in the polling place – within a few hundred feet (e.g., in the parking lot) is easy, and within a half-mile with a rudimentary antenna built using a Pringles can. Further, there are no logs or other records that would indicate if such a thing ever happened, so if an election was hacked any time in the past, we will never know" (Epstein, 2015).

WinVote was not the only model in use, but it has become one of the most noteworthy disasters in the electoral verification system. After it went out of business, its domain was swallowed by a Chinese corporation. Further, the WEP

security protocol was banned in 2004 by the Institute of Electrical and Electronics Engineers (IEEE), which brands itself as "the world's largest technical professional organization for the advancement of technology." However, because the WinVote system was created and vetted in 2002, it became entrenched. It lasted as long as it did because many (correctly) surmised that regardless of the system, hackers would always try to crack it. Dave Bjerke, the Director of Elections and General Registrar of Voters for the city of Falls Church, Virginia (where the WinVote security scandal surfaced) responded directly to Epstein's critique:

> "From an election administrator's vantage point, all voting equipment is hack-able. Nothing that we will ever get will be certified 100% secure from all outside forces. Therefore, we must build processes above and beyond the voting equipment to ensure that any nefarious acts can be caught to the best of our ability. We all agree that these machines were flawed, but can we also agree that all machines ever used by election administrators will also be flawed to a certain degree?" (Bjerke, 2016).

After spending more hours than I care to admit crawling through the transcripts of tense comment threads, it became clear that "flawed" is an understatement. Most of these dialogues focus on one theme: to what extent are elections hackable? Some veered into technical weeds, and the 'parking lot hacker' scenario captured much attention. In response to whether the polling station's WiFi signal would indeed be strong enough to reach from across the street, others asserted that an empty can of Pringles may double-function as a makeshift antenna.

One transcript of an eloquent debate between Epstein (analyst) and Bjerke (politician) ended with approval from the internet masses for Epstein's work in securitization and a Bjerke licking his pride doing his best to triage public relations damage. Before WinVote's decertification, a high schooler with no budget could

manipulate an entire database (or several) from their bedroom. An amateur with $50 of hardware could automate the process by hiding a box the size of a cigarette pack within the WiFi range of the polling station. They would then have the capacity to manipulate the entire database with even less effort. From a longer-term perspective, a hacker could also easily infect a USB drive with software that, once connected to the central server (responsible for vote total tabulation), could then re-infect other machines once they were reprogramed for other elections from the main server. This led to another lengthy debate about central databases and the anonymity of the primary server ("Master") per each polling place. Schneier, a technologist, notes, "with the possible exception of figuring out the WEP password, [this] requires any technical expertise. In fact, they're pretty much things that the average office worker does on a daily basis" (Schneier, 2015).

The counterargument (in favor of existing systems being not perfect but secure enough) asserted a doctrine of *security by obscurity*. Because 'only' the manufacturers and administrators knew how the system functioned, these same proponents argued it would take a long time before a random hacker acquired the information necessary to break through 'phase one' (the WEP). But… is it wise to trust manufacturers? (Though we'll dive into this later, the short answer is *no*). Thus, "security by obscurity" is widely considered ineffective because it pins too much of the outcome on hoping that a hacker will either (1) not attempt or (2) not find what they are looking for. So, while accessing the WEP does present a slight barrier and 'hiding' the central server might help protect the centralized database, this approach is an idealistic and passive defense, not a proactive strategy.

It's worth noting that among the many brands of DREs, WinVote is among the easiest to scrutinize. However, since WinVote was decommissioned in December

2015, several other models (beyond Diebold, E&S who dominated through 2009) have surfaced (White et al., 2022). Though current systems are improved, they are not perfect. In 2021, the Heritage Foundation identified 1,332 proven cases of voter fraud resulting in 1,145 criminal convictions, 38 civil penalties, 99 diversion program cases, 23 judicial findings, and 17 official findings (Heritage Foundation Voter Fraud Map, 2021).

The most common types of fraud include false registrations, fraudulent use of absentee ballots, buying votes, ballot petitions, forgery, ineligible voting, voting under the name of legitimate but deceased voters, impersonation fraud at the polls, multiple registrations for the same election, altering the vote count, manipulating the actual vote count at the percent, illegal "assistance" at the polls, coercion or intimidation of elderly, disabled, marginalized, or non-native language speaking voters (Election Fraud Database, 2021; Alvarez et al., 2009). When electronic systems are disrupted, denial-of-service attacks and malware become a heightened concern (Alvarez et al., 2009; Casey et al., 2019). The strategies used by various hackers, novice and elite, made the security of the hardware used until 2015 look mediocre and laughable. If this stance seems unfair or implies that I am attacking yesterday's technology by today's standards, I am not. I am criticizing yesterday's technology by yesterday's standards. Commenting on a cybersecurity study led by computer scientists at Princeton, researchers came to this conclusion:

> "[T]he machines that Americans use at the polls are less secure than the iPhones they use to navigate their way there. They've seen the skeletons of code inside electronic voting's digital closet, and they've mastered the equipment's vulnerabilities perhaps better than anyone (a contention the voting machine companies contest, of course). They insist the elections could be vulnerable at myriad strike points, among them the software that aggregates the precinct vote totals, and the voter registration rolls that are

increasingly digitized" (White et al., 2022).

From a system-wide standpoint, we find apparent vulnerabilities in the hardware (machinery) and software (program) components of existing e-voting system technology, production to application. Despite the best efforts of national and international organizations, the negative impacts of insecure elections are unresolved and worsening.

Updating to a more recent operating system (than Windows 7) is an excellent place to start but by no means sufficient. It's a band-aid solution considering that the most profound flaws (vulnerable web connectivity and centralized sitting-duck data) are infrastructural. From a historical perspective, traditional voting systems were not inadequate because of their simplicity; they buckled beneath the demands for better speed and scalability. (Again, structural features are critical). Given the extreme flaws of contemporary EVM tech and tabulation model, some might feel nostalgic for re-prioritizing paper ballots. (Today's hybrid system treats paper and DRE options equally). However, even if widespread campaigns changed the tide of public perception that, in fact, paper ballots are preferred, those paper ballots would *still* be digitized, and their data centralized at some point. Paper ballot voting — in today's world — does not exempt us from web connectivity concerns. It pushes them back several steps, removing them from sight, but the underlying problem still exists. Thus, the rise of interest in alternative vote technology arises from an acknowledgment that neither of the existing methods genuinely satisfies the needs they were designed for.

These structural flaws have inspired the search for alternatives in much the same pattern that unfolded from 1848 to 1989. From Smith, Bowerman, and Monaghan to ITT Bombay, engineers pioneered experimentations that enabled

pocketed experiments to take place in municipal elections around the world. Federal election systems adopted such systems after heavy vetting on a localized scale. Although the technology new policy must confront is unprecedented, the rhythm of this adoption — sporadic pilot testing and eventual integration at the federal level — is a pattern that's already played out. If history is any guide, the (legitimate) concerns presented are likely to pose only a minor obstacle in the eventual adoption of blockchain for citizen registry and public services — wherein voting infrastructure is just one part of the wider network (responsible for linked personal data management with other genres of public administration).

At first glance, it might even be difficult for some to understand why we haven't transitioned to a blockchain-based system already; the technology to do so has been at our fingertips for nearly a decade. Though part of this hesitation is due to tangible logistic and security concerns, another reason for lagging development might be attributed to the pigeon-holed conceptions of blockchain for alternative Fin-Tech only. Blockchain and cryptocurrency are not the same. Moreover, rhetoric synonymizing a framework (blockchain) with a use-case (cryptocurrency) has conceptually undermined our collective ability to understand the deeper implications for the future of how we curate information sharing.

Blockchains architect the space in which digital data transactions — financial or otherwise–can happen. Although they make up the backbone of the cryptocurrency market, they can frame other data management systems as well. Moreover, it's also essential to recognize that they are a "they." Though all blockchains function according to the premise that every validated transaction is a "block" linked to the block before and after it, thus "chained" together, the nuances of individual blockchains bear significant ramifications. (More on this when we

discuss the case studies).

It's essential to recognize that Blockchain is the framework within which coins are traded, like Bitcoin and others. They are *not* the same. This would be like saying "Google is the internet" when Google is an entity that lives courtesy of the space architected by the internet. If one were discussing it in cellular terms, Google would be an organelle, not the cytoplasm. Blockchain, like the internet, is more comparable to "the cytoplasm" in this analogy.

A blockchain is a data structure that harbors all transactional records ever conducted on the chain. Its chief characteristics are securitization, transparency (all transactions are visible, but transactors are anonymous), and decentralization (Pratap, 2018). As the name suggests, each transaction is recorded and stored as a "block" (MLSDev, 2019). Furthermore, every block must achieve consensus in that all computers (nodes) on the network must verify the transaction's validity. After this verification, it is recorded on the ledger is recorded on the running ledger with a numeric identity (i.e., not linked to a name) that contains both a numeric timestamp sequence and an algorithmic fragment of the transaction prior. For years, international regime theorists have cited "an embedded sphere of consensus" as a starting point for conflict reduction (Nye and Keohane, 1989). Though most of these examples revolve around international trade, aviation standards, and development aid, this zonal concept applies to every sector where common rules and regulations can be found. Could this apply to future blockchain-based e-voting systems? It's possible. Particularly if nations use a localized registry (i.e., data remains within their borders) but that is anchored to an international network operating on a consensus mechanism.

If every vote cast can be viewed as a "transaction," is it too far from the realm

of possibility to state that Blockchain can frame electoral accounting systems? It's workable. One can imagine a blockchain vetted system operating alongside traditional verification mechanisms and (perhaps) overtaking them. Can a blockchain-based e-voting system perform better than the status quo without introducing more risk than reward?

This question of whether blockchain can reduce electoral corruption opens a pandora's box of puzzles about personal data management, cybersecurity, technocracy, and public policy, among others. The trade-off (prioritizing alternative tabulation methods) presents tempting advantages. Why verify a result a handful of times when millions of nodes can instantaneously validate each vote cast? Why fumble with expatriate and military ballots cast overseas when votes can be identifiably cast at the expense of safety and anonymity? Why deal with mail-in ballots and suffer the delays of tallying them all at the last minute (Library of Congress, 2021)? Nonetheless, these conveniences still come at a cost. What stands to be gained and lost from implementing blockchain-based e-voting systems?

Further, what other opportunity costs exist for not anticipating the legislature and policy needed to regulate these inevitable developments? When I began this research, there was relatively little scholarly literature on the topics we'll be discussing in this manuscript. Most of what I learned (beyond standard research) came from personal conversations within the private sector or front-end, back-end, and full-stack developers on the market. During the first research phase of this project, I investigated anecdotal insights from these discussions. This led me down the rabbit hole to discover more concrete databases describing the industry trends indicated by the persons I talked with. Most of the time, these insightful 1-1 interactions were validated. In the second year of my research, the empirical

literature on blockchain-based e-voting systems mushroomed from near-nonexistent to proliferating.

More telling, real-world pilot projects (most implemented after 2018 with the exception of Estonia) have not fizzled but flourished. This flurry of life-scale beta-testing in pockets around the world mirrors, in small part, emergence patterns of past tabulation tech just prior to widespread global adoption. It also illustrates that blockchain-based alternatives, though not perfected, are possible. What remains to be seen is how invariable hiccups will be addressed and what repercussions will emanate from these vulnerable moments. In the following section, we'll review Estonia's BitCongress and X-road, Russia's Exonum, Switzerland's uPort on the Ethereum (ETH) chain, Japan's UnilayerX (Layer X) partnership, and the sporadic state-level experimentations with Amazon's AWS and Microsoft's Azure distributed across Hyperledger (HF) sprouting in Virginia, Utah, and Colorado of the USA.

CHAPTER 3

THE SCHOLARLY DEBATE ON BLOCKCHAIN VOTING

When it comes to implementing blockchain-based e-voting initiatives, scholars and laypeople alike are split about what should be done. Though there is little disagreement about whether there is a problem, there is extreme discord regarding *what* should be done. Though Hassan et al. and others created three major categories (traditional, e-voting, and blockchain) to itemize differing needs and vulnerabilities of these respective voting systems, Park et al. identify not three but four main categories. This organizational logic may allow for greater analytical flexibility in the long run. Their criteria are bifurcated by two key features: in-person versus remote.

Table 1. Four Categories of Voting Systems

	In-person	**Remote**
Voter-verifiable paper ballots[3]	Precinct voting	Mail-in ballots
Unverifiable or electronic ballots	DRE[4] voting machines	Internet/mobile/blockchain voting

Source: [Park et al., 2021]

Their research team labeled the top-row as "software-independent" and, accordingly, more resistant to tamper than the susceptible "software-dependent" bottom row. Where the lines get blurry is in the bottom left corner. In this quadrant, all internet-based voting methods are cast in the same basket with prospective blockchain-based e-voting mechanisms. This is potentially problematic because their encryption and data storage methods are incredibly different (we'll open this topic later on). For the

moment, however, it is worth noting that there are several conflicting lines of debate. One of them splices down the middle— dividing those who favor in-person voting methods over remote voting methods regardless of the technology used (paper or otherwise). A second debate emerges on the horizontal division of this table— between voter-verifiable paper ballots and unverifiable (electronic) ballots. However, this project zooms in one step further, problematizing the unverifiable category twice. First, we'll address the weakness of DRE voting machines relative to any alternative whatsoever. Then we look at those alternatives in the hopes of determining the best one. In other words, though the project will cover a little of all categories, the lower right quadrant (remote/unverifiable) will receive special analytical attention throughout this research.

Our focus is less on whether digitization is normatively "good." Rather that it is inevitable, and therefore in need of policy attention. Avoiding analytical confrontation is worse than trying to assume away the problem. Moreover, paper options are not always accessible, particularly given higher rates of ex-patriated citizens and intermittent pandemic dynamics requiring social distance. Therefore, we cannot ignore developing safe and secure digital options in this era— even if paper might be preferable. For those who found extreme dissatisfaction with DRE-based or other inadequate internet or mobile voting options, blockchain has garnered incredible enthusiasm, citing:

> "… great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations— voters can vote from wherever there is an Internet connection (Jafar et al., 2021).

Likewise, Gonzales et al., who problematized the concept of centralized voting,

shares their optimism. According to their research team, permissioned blockchains may "present an alternative for participatory management processes, such as electronic voting, focusing on the following core values: trust, transparency, and immutability" (Gonzales et al., 2022). Among the most significant reasons for this is that blockchain turns upside down all previous information sharing, verification, and securitization mechanisms. This affects not only the digital finance industry but any system relying on database management. In today's world, that can apply to any large-scale system regardless of industry or sector, from private enterprise to government.

As a researcher, "hype" is generally seen as a red flag signaling empirical bias. And in some academic manuscripts— even highly technical ones like Gonzales et al. and Hassan et al., where this enthusiasm is not self-corrected by thorough counterargument dismantling one's own position— blind, unrelenting enthusiasm can become a turn-off. However, regardless of whether it's the right moment for policy to adopt blockchain as an emerging norm, the structural implications of the information transaction on the blockchain are indeed phenomenological.

In the pre-blockchain era, all previous conceptions of a 'database' relied on compiling a central pool of data information. These databases existed beneath the managerial influence of one (or a tight group) of authority. In other words, the power of this data was highly consolidated. Thus, blockchain is an attractive option because it can scale to accommodate large user populations and fortify this ever-growing database, all without surrendering authority over that data to anyone. Buoyed by these prospects, an increasing bulk of developers and researchers are extremely optimistic. For example, Gonzales and his team conducted their analysis using Hyperleger Fabric (HF), a type of permissioned decentralized ledger technology

(DLT) founded by the Linux Foundation. It is both open-source and 'enterprise-grade,' meaning that it can integrate smoothly within existing infrastructure "with minimum complexity and offer transparent proxy support" (Gartner, 2022). Their work supports others (such as Jafar et al., 2021; Polyakov, 2022; Polge et al., 2021; and Alessie et al., 2019) who are enthusiastic about the prospects of using blockchain to reinforce electoral tabulation systems and other aspects of digital government.

Though they are not alone in these conclusions, not everyone shares this excitement. Others assert that to go down the rabbit hole of blockchain-based civil services (elections among them) would be to go from bad to worse (Park et al., 2021; Wofford and Halderman, 2016; Schneier, 2004 and 2022; and Specter et al., 2022). They acknowledge that the current system is bogged down by "serious failures," including, but not limited to, "attacks that are larger scale, harder to detect, and easier to execute than analogous attacks against paper-ballot-based voting systems" (Park et al., 2021). Is it fear-mongering to point to existing threats as a valid reason to assume greater risk—to dive head-on into a technology with greater unknowns? The responses are split down the middle even amongst highly qualified academicians, researchers, analysts, and security specialists.

3.1 Blockchain basics

We'll discuss this bifurcation further, but it would be mute to dive in too deeply without providing a technical overview of blockchain technology and *why* it differs so greatly from yesterday's data transaction and management systems. A blockchain (or a chain of specific blocks of information) is both a database and a peer-to-peer network. We can also describe it as "a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized."

(MLSDev, 2019). Because it is public (wherein all users are anonymous), it can be much safer than private systems (where users are not anonymous). Comparing blockchain-based systems versus traditional databases, we can itemize these critical differences within four general categories: network model, data structures, advantages, and types of blockchain structure.

Table 2. Blockchain vs. Traditional Data Systems

Network Model	***Data Structures***	***Conventional Benefits***	***Blockchain Structure***
P2P Network (rather than Client-Server)	Pointers Linked Lists	Cost Reduction Data History Data accuracy, verification, and security	Public Private Consortium Hybrid

Source: [Author, 2022]

3.2 Network model

What's the difference between a client-server network and a P2P Network? As the name suggests, a client-server network differentiates between "client" and "server" entities. The centralized server stores and manages all data. The only way to be an administrator is to have explicit permission. This database focuses on centrally managed information sharing and distribution. (The World Wide Web is structured according to this). Although client-server networks may be more stable in some respects, they tend to be more expensive than P2P networks. Though it responds to service requests by the client, authority rests in the curator of the server.

Figure 5. Client-server vs. P2P network
Source: [MLSDev, 2022]

In contrast, a P2P network does not differentiate between clients and servers. Treated as identical, they are all called nodes. Because every peer has its own data, every node can initiate and respond to services. Rather than information distribution (a top-down activity), the aim of a P2P network is connectivity. Though less stable if the number of peers increases beyond a certain threshold, it is less expensive to maintain than a client-server network. P2P is the hallmark of decentralization.

Thus, a blockchain (or a chain of specific blocks of information) is both a database and a peer-to-peer network. We can also describe it as "a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized" (MLSDev, 2019). Furthermore, because it is public (wherein all users are anonymous), it can be much safer than private systems (where users are not anonymous).

3.3 Data Structures

Two critical data structures, known as pointers and linked lists, help maintain the sequence of transactions. In other words, these elements keep the blocks on the chain in order. Every Blockchain uses pointers as a reference. Quite literally, they point to the exact position of another variable. Zooming out, linked lists represent the sequence created by ordered blocks. Every block is stamped with specific information. The data in this stamp includes links to the correct next block in the sequence, and it connects to that block with the help of a pointer. (Side note: The first block is “pointless” —it doesn’t need a pointer and does not have one. Conversely, a hypothetical “final block” may have a pointer that is actually pointless—it points to nothing).

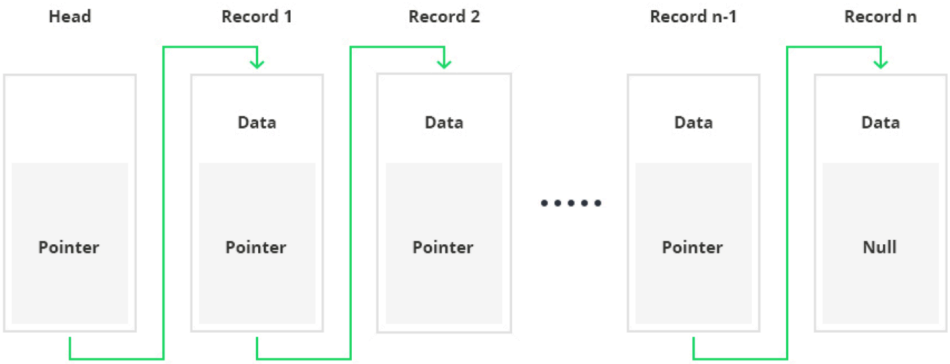

Figure 6. Blocks and data pointers
Source: [MLSDev, 2022]

These concerted connections create a block, a batch of recorded transactions. This data block is the basic unit of the Blockchain. Each block is encoded with information about the block preceding it and the one to follow. A complete block is a permanent record that simultaneously accounts for past transactions, details the

current transaction, and sets the stage for future transactions (Frankenfield, 2020). For example, A Bitcoin (BTC) block can contain up to 1.31 MB allowing for a transaction averaging about 500 bytes (Centierio, 2021). Each complete block acts as a leger and a chain link. Strung together, we have none other than the "blockchain" (Frankenfield, 2020).

3.4 Conventional benefits

For all the complexity of any given chain, the fundamental reason why Blockchain has taken hold in so many theatres beyond digital finance is that it offers conventional business benefits that are tough to top with any other technology. Among the many advantages, a few critical assets are at the top of the list: cost reduction, data history, data accuracy, verification, and security.

3.4.1 Cost reduction

While gas fees do incur costs for users, blockchain platforms operate with reduced friction costs relative to other centralized (client-server) networks. "Gas Fees" are transaction fees. Every time a user makes a transaction, they essentially "pay" miners on the blockchain protocol for their transaction to be added to the block. The logic is that the coins would not be accessible to the users if the miners had not done the dirty work of mathematically bringing these coins to the marketplace via solving the chain's algorithm. Despite gas fees, the costs on blockchain-based exchanges are so reduced relative to traditional means that some claim it is disruptive to traditional banking (Gan et al., 2021). Regardless of whether one is in favor or opposed, others note "90% of members of the European Payments Council believe blockchain technology will fundamentally change the industry by 2025" (CBS Insights, 2021).

Why? Blockchain essentially replaces the expensive 'middleman' (traditionally, a bank handling the transaction) with a " smart contract" (a computer code embedded with a self-executing protocol verifying the terms of the buyer and seller) (Khan et al., 2021). "Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism" (Frankenfield, 2020). In addition, the smart contract allows blockchains to run on a *permissionless* basis. In contrast, the traditional financial system relies expressly on permission. For example, to send an international wire transfer from the United States, the transfer passes through many hands— each taking a cut. On top of a flat rate wire transfer fee of, let's say, $25, there can be up to 7% of the transfer sum in additional fees. This doesn't include exchange rate fees (the sender is responsible for those too). Previously, the silver-bullet argument for this extortion and inefficiency has been security. With the capacity to engage smart contracts, it is possible to maintain security while facilitating cost reduction, reducing transaction time, and keeping a more detailed record of data history.

3.4.2 Data history

To date, Blockchain is the only technology that boasts the ability to "render transactions traceable, transparent, and irreversible" (Frankenfield, 2020; Khan et al., 2021). As mentioned, each block is not only embedded with data from past and present; its numeric identity primes the next unit in the sequence. Thus, the algorithm produces a pattern "with every block containing the hash of the previous block to create a blockchain" (Crosby et al., 2016). In addition, each transaction must be verified by every node on the network before being recorded, i.e., achieving

consensus on the network.

Any device connected to the blockchain network qualifies as a node because it implicitly contributes to the constant updating of information on the chain. Servers, computers, laptops, online or desktop wallets, and mobile phones can all become nodes. However, not all nodes are created equal. There are three types of nodes, each serving a unique function to the survival and maintenance of the chain: miner nodes, full nodes, and light nodes (see appendix). We'll focus on full nodes in this discussion, which can store the blockchain's complete information. These full nodes can act as core servers across decentralized blockchain networks (Casino et al., 2019; SEBA, 2021).

Thus, it plays an invaluable role in validating and verifying real-time transactions. Alongside validating new blocks, nodes maintain transaction history (essential for a system linked via an ongoing chain) and update other nodes with the latest information (all nodes must agree before recording a transaction/validating a block).

Though the entire history of a blockchain *can* be stored on a single full node, it is not ideal. More nodes on the network mean more decentralization, more significant verification, and more resistance to technical issues such as power outages or system failures. "The core benefits of nodes are to ensure the data being held on the blockchain is valid, secure and accessible to authorized parties" (SEBA Bank of Switzerland, 2021). End-to-end working node transaction simply means that the transaction model is dependent on the full agreement (consensus) of all active (working) nodes constituting the network. In the same vein, end-to-end encryption (E2EE) implies messages relayed will be private to all but the sender and receiver, i.e., it's encrypted from start to finish.

For example, if a user has X amount of BTC and wants to send a Y portion of it, every full node on the network will confirm every step of that transaction. All sending full nodes (associated with the sending wallet) will confirm (1) that there are enough coins to make the transaction, and (2) receiving full nodes (associated with the receiving wallet) will validate the transaction upon receipt. The block (created by miners to verify this transaction) will then be verified by proof of work (PoW), one of two vital 'proofs' for improving data accuracy.

3.4.3 Data accuracy, verification, and security

The Security of any blockchain depends upon consensus mechanisms to validate transactions. It maintains data accuracy, verification, and security via cyber-security strategies based on Sybil Deterrence Mechanisms (SDMs) (Casey et al., 2021). A Sybil attack is a type of cybersecurity breach where one attacker pretends to be many simultaneously, which is risky in a P2P network dependent on consensus models. There's an interesting niche of work on "deception, identity, and security" with respect to "the Mathematical Game Theory of Sybil attacks" that reads as if it's flown out of a science fiction novel (Casey et al., 2016). However, for now, we'll focus on the two strongest SDMs relevant to the blockchain world: Proof of Work (PoW) and its alternative, Proof of Stake (PoS).

Proof of Work is a consensus protocol involved in mining. It is used for (1) validating transactions and (2) mining new tokens (Al Ahmad et al., 2018). As miners validate transactions (adding new blocks to the chain as they do so), their productivity makes it ever so slightly more challenging to mine the next block. (Note: For anyone familiar with the SHA-256 hashing algorithm, this applies here) (Gilbert et al., 2004). The key uses of PoW are cryptocurrency mining, validating

transactions, and mining new tokens (Al Ahmad et al., 2018).

PoW enables peer-to-peer (P2P) transactions to happen on a permissionless basis (i.e., no trusted third party necessary) (Khan et al., 2021). The PoW consensus algorithm is a cryptographic zero-proof model where a specific set of computational evidence is offered by one entity (the prover) for verification by the other parties (Jakobsson and Juels, 1999). It takes more computational effort to provide this information than to verify it. In 1993, the PoW concept was created to mitigate denial of service (DoS) attacks—cyberattacks— long before blockchain ecosystems existed (Prakesh, 2016). However, because PoW demands such high computing power, it has also been heavily critiqued. Though it is still the verification method of choice by crypto giants such as Bitcoin (BTC), others have taken active steps to transition towards a smart-contract verified PoS verification model (McQuaid, 2022).

Thus, Proof of Stake (PoS) arose in response to PoW as an alternative. In terms of mining, PoS allocates mining power according to how many coins a miner already has (Al Ahmad et al., 2018). In other words, PoS selects validators on a proportionate basis: the more significant their holdings on the network, the greater their role. Unlike PoW, it does not incentivize massive energy expenditure. Cardano, Solana, Polka-dot are all PoS examples. Ethereum 1.0 was initially designed in a PoW model. However, Layer 2 (Ethereum 2.0) is slated to be PoS. It's being developed as a PoS to accommodate more transactions while using less computing power.

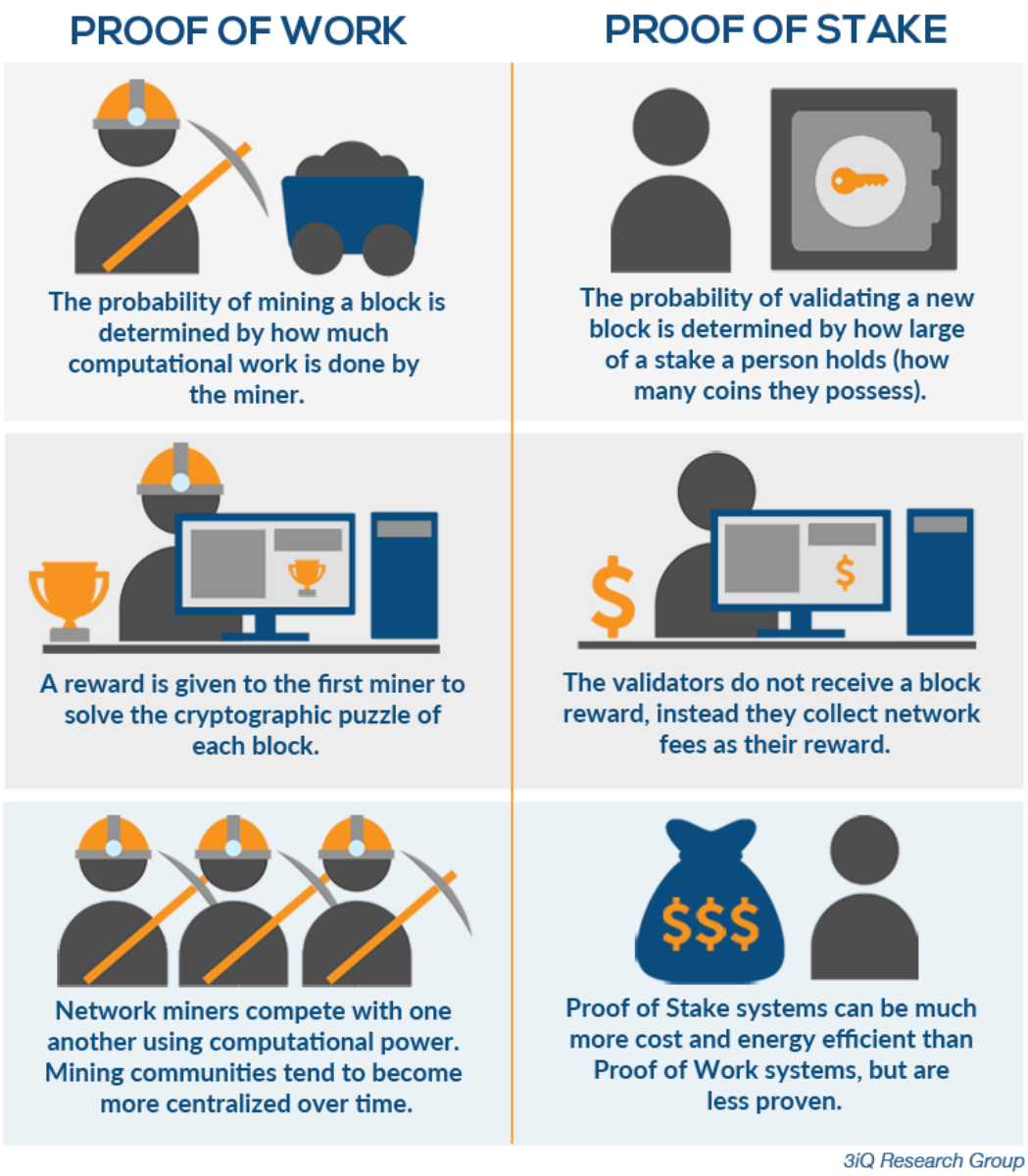

Figure 7. Proof of work (PoW) vs. proof of stake (PoS)
Source: [3iQ Research Group; Digital Asset Management, 2022]

Smart-Contracts are digital agreements in the form of a software program that automate processes according to preset conditions. These programs are stored on the blockchain and run only when triggered by these predetermined conditions. Because these procedures are software scripted, there is no intermediary wages to pay nor processing time lost, as there would be in a traditional system. The smart-contract protocol automatically engages and executes.

> "Smart contracts work by following simple 'if/when…then…' statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified…To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the "if/when...then…" rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes" (IBM, 2022).

Each time a function in the contract is completed, the blockchain updates to reflect this. Because the predetermined conditions function as a 'trigger' these can be seamlessly created into a workflow, where the completion of one data exchange or transaction becomes the catalyst for the next action to begin. These are critical to the PoS verification model. Moreover, because an abundance of templates, online tools, and other web interfaces exist, an original developer isn't necessarily needed for an organization or entity to optimize smart contracts to their needs.

We'll dive deeper into these and other Sybil Deterrence Mechanisms later in the content—so, keep it on the backburner for now. The biggest takeaway is that PoW and PoS play a crucial role in the data accuracy, verification, and security advantages Blockchain provides. This sub-field of advantages is stitched into a broader fabric. However unconventional Blockchain might be (at least by many contemporary business standards), it can yield conventional business benefits: cost reduction, data history, data accuracy, verification, and security improvements.

Though Blockchain is still underutilized, some private and public sector entities are picking up the torch. Of course, how they do so depends on the type of Blockchain they use. Still, this post has already continued for much longer than anticipated. Next, the spotlight will shine on the main Categories of Blockchain Structures (public, private, and consortium) and their use cases.

3.5 Categories of blockchain structures

There are four general types of blockchain structures: public, private, hybrid, and consortium. Public chains are decentralized (ownership is permissionless and dispersed). Private chains are centralized (ownership is permissioned and centralized). Consortium chains embody public and private chain properties. Below, we'll outline each chain type, provide a few examples, and open the pros and cons of each. Hassan et al. (2022) created a figure to depict the different types of blockchains.

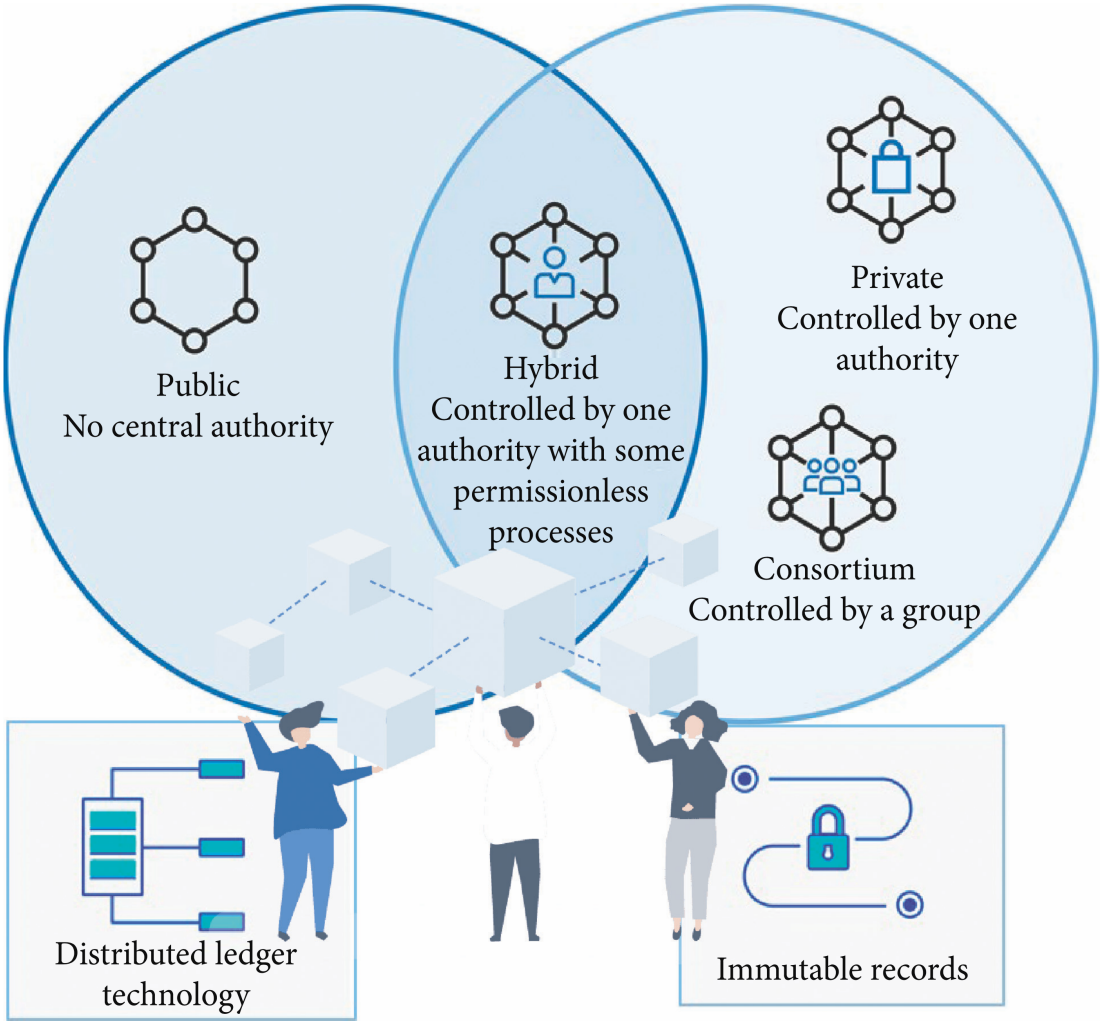

Figure 8. Types of blockchains
Source: [Hassan et al., 2022]

Distributed ledger technology (DLT) means that ledger data is located in different

places (i.e., distributed or *de*centralized), not one (centralized). Because this power distribution technique is embedded in the system infrastructure, it is sometimes referred to as “liquid democracy” (Hassan et al., 2022)

3.5.1 Public blockchains

The first, as the name suggests, can be joined by anyone. Likewise, everyone has equal access to participating in the core activities of the Blockchain. Core activities include any procedure directly affecting the functioning of the chain from coding to staking. Those involved in coding are probably familiar with The Linux Foundation, a nonprofit tech consortium promoting open-source software development (Chelkowski et al., 2021).

Though public and private changes are similar in many ways, the key blockchains fundamentally change implications toward the anonymity of the users on the network and who can participate in the core activities sustaining it. For example, Bitcoin (BTC), Ethereum (ETH), and Litecoin (LTC) are all public chains. All coin giants of the crypto world all adhere to public blockchain principles. Data cannot be changed once validated— ever.

Because public blockchains are open-source and the ledgers are visible, users can retain their anonymity while enjoying network transparency. Nothing happens behind closed doors, but individual identities aren’t sacrificed at the altar to maintain this transparency. All data is trustable, transparent and secured without the use of intermediaries. There are, however, a few downsides. Public chains are riddled with scalability problems, transactions speed sometimes suffers, and they consume immense amounts of energy to maintain relative to other networks.

3.5.2 Private blockchains

A private blockchain is a centrally managed *permissioned* network (a network one must be invited to participate in) (Polge et al., 2021). This exclusivity comes with advantages and disadvantages. In addition to higher transactions per second (TPS) scalability, private chains are more efficient and responsive in certain circumstances.

However, there are some significant trade-offs: anonymity and transparency are sacrificed. Because users forfeit their privacy and transactions are not visible to the public, achieving trust is near impossible. Private chains are also less secure than public networks. Likewise, managing (or administrative) entities can retrospectively alter data entries in a private network," and no one outside the administrators will know.

This creates more than a few risks. Among the disadvantages (for users) of centralization, compromised security, control, censorship, and regulation open opportunities for data manipulation by the managing authority. This poses a fundamental threat to the credibility of the leger and, potentially, the safety of the users on the chain. In either case, these parameters at least seem straightforward—open or closed, non-permissioned or permissioned. That holds, at least until we dig deeper into the concept of "permission." Consider the two questions below:

i. Can a private blockchain be open source?
ii. Can a permissioned blockchain be open source?

The answer to the first question is straightforward, no. However, it might surprise you to hear that the answer to question two is *yes*. The lesson here is that private and permissioned blockchains are *not* the same (Seth, 2021). It's the same as saying a

square is a rectangle, but a rectangle is not a square. Private blockchains necessitate permission. In other words, only verified participants are allowed, and the administrator has full autonomy to override, revise, or omit transaction entries on the blockchain ledger. A permissioned chain integrates characteristics from both. Anyone can join an open-source, permissioned after standardized identity verification. The client/software can verify that the clients/nodes connecting to the chain at any given moment have all been verified upon entry before connectivity.

3.5.3 Consortium blockchains

Though they most closely resemble permissioned chains, consortium blockchains stand in their own category. Sometimes called "federated" blockchains, consortium chains are typified by a group of private entities engaged in the same field collaborating to run a chain. The data-sharing platform they create is neither centralized like a private chain nor truly public. According to the Blockchain Council:

> "In this type, there is more than one central in-charge, or we can say more than one organization involved who provides access to pre-selected nodes for reading, writing, and auditing the Blockchain. Since there is no single authority governing the control, it maintains decentralized nature" (Blockchain Council, 2021).

Because of its hybridity, consortium chains are ideal for organizational collaboration. They are easily scalable, very secure, and efficient. They also offer extreme advantages when it comes to customization and managing resources— a major selling point for private enterprises. Despite these benefits, however, consortium chains cannot compete with the when it comes to the transparency and anonymity offered by public chains. Some examples include Hyperledger Consortium (and the

Performance and Scalability Working Group), Energy Web Foundation (focused on de-carbonizing power grids), IBM Food Trust, BankChain, B3i, and China Ledger.

3.5.4 Hybrid blockchains

Some chains appear more complex because, though they might operate on a consortium basis, they can behave in way that is private and permissioned—or not. Because control is consolidated within a single organization its optimal for private enterprises seeking. However, unlike a true private chain, hybrid chains involve some form of public oversight (Wegryzn and Wang, 2021). Without that public involvement, certain transaction verifications might be impossible to verify. This is the fundamental distinction between hybrid chains and their permissioned or consortium counterparts.

Some hybrid examples include Hyperledger Fabric (HF) (produced by the Linux Foundation) and Hyperledger Sawtooth. Often, hybrid platforms can flow between private and consortium, such as the public affairs software, Quorum (Polge, 2021). It's designed for private use (wherein one member owns all nodes) however, it can be adapted to include multiple owners who would each own part of the network (a distribution of nodes amongst a select few).

3.6 Implications on further development

As with anything, pros and cons exist for each chain type, with no strict, standardized "best option." It's entirely subjective to the needs of the individual or entity, depending on the network. As an individual, public blockchains provide the greatest transparency and protection. As a business, it isn't. Such a situation is ripe for ongoing design-in-use analysis tracing the spoken and unspoken compromises made by both parties — designers and users (Aoussat et al., n.d).

Fundamentally, there are two innovative, ideologically opposed paths occurring side-by-side. One prioritizes the user. The other is driven by investment. It's safe to say that the trajectory of this field will have significant implications on the individual privacy and data rights of present and future users on these networks. In ages past, rights-related decisions would have been handled in the courtroom. However, it's unlikely these determinations will even surface into the legal realm before they are decided. Instead, conclusions will be made indirectly via funding flows and heavy capital pumped into projects preferential to business interests over human rights interests. For instance, suppose project X and project Y both need Z amount of funding to lift off the ground. Project X protects user rights but doesn't satisfy the sponsor's needs and wants, while Project Y does little to safeguard users but capitalizes on the sponsor's demands; which project will receive funding? Project Y. Which project might have been better for society? Project X. Ricardian principles of comparative advantage might never have the opportunity to unfold organically if the 'market winning' selection is determined before users even realize there was an option (Ricardo, 1817).

If we accept the assumption that capital articulates innovative direction, the future of the field is likely to be influenced by proportional investment, where giant

entities hyper-fund certain developments favoring their business interests over the individual. This splinters against the grain of classical liberal values (Doyle, 1983) in exchange for aspects of corporate capitalism (Kotz, 2008).

3.6.1 On-chain governance: key players in development and upgrade protocols

Another key feature to remember is that blockchains, once created, are not fixed. Instead, they evolve according to an adaptive process called "On-Chain Governance" (Pelt, 2020). This reflects the shifting needs of users (those transacting on the chain), the actions of miners (minting new coins into existence), and the interests of developers (responsible for algorithm maintenance and development) and stakers.

These chains evolve via upgrades to the software defining the platform. However, one of the most phenomenological aspects of these upgrades is that they are not conducted behind closed doors. Instead, each upgrade can occur only to a specified set of rules that outline democratic procedures that must be met before changes are implemented. This set of rules is called an "upgrade protocol." They are embedded with concern for the representation of the individuals sustaining and using the network indicates that they operate according to "democratic consensus" principles. That these built-in consensus mechanism operate autonomously (absent a central governing authority) makes it an unprecedented structure for scholars to theoretically quantify. Consensus (or agreement) helps avoid conflict (Nye and Keohane, 1989). But what happens, in a blockchain environment, when consensus is lacking?

3.6.2 Hard and soft forks

Where consensus cannot be achieved or when there is a significant change in

protocol, we might see the developers split. One group continues to develop the software along the original protocol track while the other group moves forward independently from that juncture in a different direction. According to CMC Markets, “A hard fork is a radical change to the software which requires all users to upgrade to the latest version of the software. Nodes running on the previous version of the software will no longer be accepted on the new version” (CMC, 2022). (Further information on the figure below can be found on a platform called “Etherworld”).

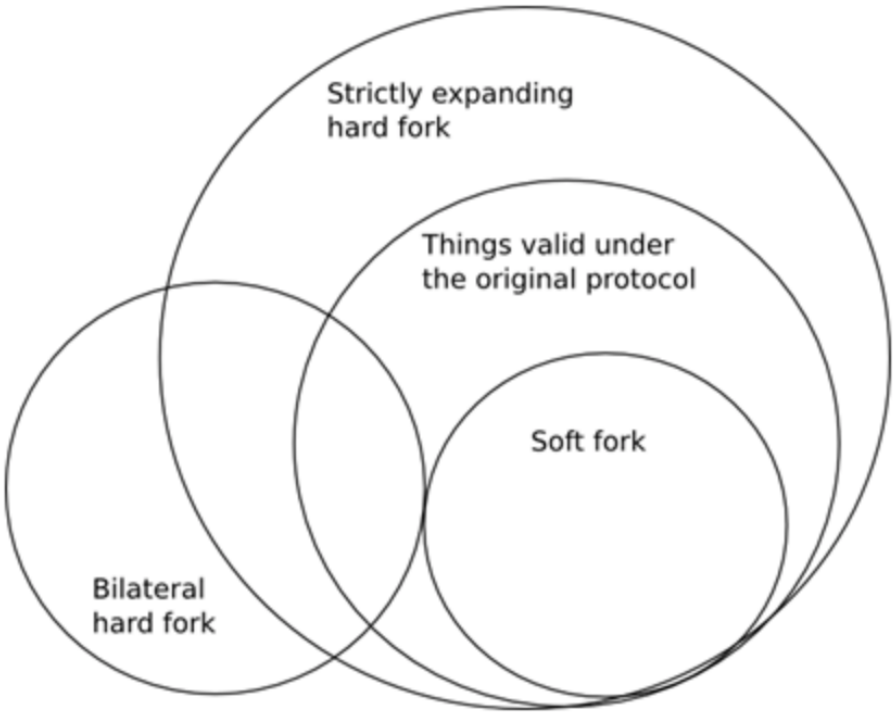

Figure 9. Fork types
Source: [Etherworld, 2022]

Hard and soft forks (and the sub-forks depicted above) move forward according to different rule sets and trade-offs (Zhang et al, 2018). Hard forks tend to be more favorable to developers because of their malleability. Anyone furthering the project can do so without squeezing into the previous, confining framework. However,

because the hard fork (true for strictly expanding and bilateral hard forks) is incompatible with the previous system, it's necessary to install new software and nullify all previous transactions and blocks (i.e., it makes them invalid). Furthermore, because the change in the protocol can be extreme, there's a higher probability of the chain splitting again in the future (increasing risk, reducing safety). For this reason, hard fork demand prior consent from users and accepts opt-in users.

In contrast, soft forks tend to be more user-friendly. When a soft fork happens, the user-experience remains more constant, and they don't have to upgrade to remain on the chain. Likewise, no new software installation is required. Though it only allows valid transactions (past and present so long as the according with the new soft fork protocol), it doesn't invalidate all of them as a hard fork would. There's also a lower likelihood of a future chain split, making it more stable long-term. Although no consent is needed from the users, miners/validators do need to consent for the chain to move forward. There is also no opt-in option (Etherworld, 2022). In effect, upgrade protocols guide governance. Whether a chain develops sharply (hard fork) or adapts via incremental changes (soft fork) not only influences the relevance of the chain (with respect to the needs of its users) but its survival. Thus, the comparability of on-chain governance mechanisms and traditional policy development cannot be understated. "Upgrades" can be thought of as "policy reforms." Equally, "protocol" is comparable to "law." That they operate on a democratic consensus basis also illustrates how much they've borrowed from liberal institutionalism as it might manifest in the political realm. Though these protocols vary from chain to chain, that's a basic outline of how they operate.

Stepping away from the technical for a moment, let's return to the heated debate happening in the literature. Are we seeing division over the inherent

governance mechanisms used by blockchain-based systems or something else? What we find as we re-enter the scholarly debate is not that such systems are incompatible with democratic initiatives but something far more ambiguous (Pelt et al., 2020).

The crux of the arguments not in favor of blockchain-based e-voting are not unanimously taking issue with the technology itself but are against trends toward online voting options in general— blockchain being one such option.

> "There's considerable skepticism, including from renowned elections and cryptography experts, about whether blockchain is the right technology to accomplish online voting — or whether online voting is the right way to go at all. With concerns swirling about foreign interference in America's elections, many are calling on a return to paper ballots that can't be manipulated en masse" (Miller 2022).

Likewise, opposition to the concept of using blockchain technology in electoral systems is stratified: low, medium, and high. Those softly against implementing e-voting systems argue that it is an enthusiastic trend. Individuals with a harder stance in opposition to blockchain-based e-voting systems claim that e-voting (regardless of the means) is not as effective as one might expect. The relatively new term, "eParticipation," describes political engagement trends comparing online with in-person interactions (Spirakis, 2010). Some countries (Switzerland) noted no change, while others (Bulgaria) actually identified a slight decrease in voter participation (though the latter may have been because the pilot project took place in a mock setting with no real-world outcome) (Germann, 2017; Dandroy, n.d.). At almost complete odds with these results, the number of proposals to make initiatives regarding online voting has skyrocketed. "So, why the push?" they ask. The incongruence is enough to make one question whether greater digital voting initiatives would simply increase existing inequalities between the citizenry rather

than empower them. There is mixed debate about Estonia for example (Serdült et al., 2015). Lastly, those most strongly against blockchain-based e-voting fear that risk absorption costs would be borne by the voter more than any other entity.

CHAPTER 4

FIVE REAL-TIME CASE STUDIES

Regardless of which side of the debate one finds themselves on, that has not stopped pocketed experiments from emerging around the globe, nor scholars from analyzing them. Almost all these experiments emerged after the 2018 ICO boom. Yet, because only one case (Estonia) implemented a smart-contract registry and blockchain-based verification at the national level, these developments have made a smaller splash outside the dev (developer) and analytics community than one might expect. Nevertheless, it benefits all of us to look at these nascent cases because they are the only cases. Estonia's BitCongress, the Moscow city council elections (2019), municipal elections conducted in the city of Zug, Switzerland (2018), local elections in Tsukuba, Japan (2018), and scattered experiments in the United States may shape politico-infrastructural ecosystems in a way that may be difficult to reverse if it goes badly (Beedham, 2019).

Moreover, will tech-based alliances facilitate international cooperation or undermine the balance of power dynamics—or both? All hypotheticals set aside, the first question that comes to mind is: how did these real-time experiments unfold? What can we infer from their prospects of reducing electoral corruption or— at a minimum— human error.

4.1 KSI blockchain: Estonian BitCongress

Perhaps the first question that comes to mind is, how did this former-Soviet nation nestled between the Baltic Sea and the Gulf of Finland become the global frontrunner in e-voting technology? Though the country boasts a robust telecommunications and

electronics sector, many of its contemporaries do, too, so what makes Estonia different? One speculation is that Estonia was ripe for these developments not simply because her labor force is highly skilled. Estonia's population is tight. Amongst 1.3 million individuals, there are only a few hundred thousand voters. This dynamic may have helped the country scale this new infrastructure to the national level with less disruption. However, the countries with the highest notoriety for the density of skilled labor within their borders are Switzerland, Singapore, Sweden, Denmark, and Australia (Global PEO, 2021). Estonia is not on this list, and yet here we are, discussing it as a global frontrunner. Though there isn't enough available information to determine *why* Estonia became the first country to implement blockchain-based in this context, it is.

Though several countries experimented with e-voting techniques, in 2005, Estonia became the first country to host legally binding elections (Tsahkna, 2013). Because Estonia implemented a nationwide internet-voting infrastructure in 2005, the concept of introducing blockchain alternatives without compromising security may have seemed less insurmountable. Before blockchain was invented, the initial i-voting (internet-voting) system relied upon public-key cryptography. This generates a private key (per the voter) and a public key (for the central administrator(s)). The previous version of this system, though entrepreneurial, stirred concern for two reasons. (1) the interest connection could be compromised (2) it required individuals to place their trust in the integrity of the centralized system. According to the Estonian National Election Committee, five years after internet voting was normalized in Estonia:

> "The defence of the use of personal computers is that those with the knowledge, resources and access to infiltrate the computers of a large number

> of voters have no motivation to do so, and that the political forces who have the motivation cannot afford to take the risks associated with that kind of intrusion. People who conduct business and financial transactions using computers take higher risks in their everyday lives than during e-voting" (Anspur et al, 2010).

Despite the benign rhetoric above advocating to hope no one was 'motivated' to try hacking the system, the Estonian government made decisive and hasty efforts to improve the system's security in the wake of a series of cyberattacks three years earlier. In 2007, Sergei Markov, an ethnic-Russian Estonian spear-headed an attack on Estonian private sector institutions, including telecommunications operators, half the country's major media outlets, two national banks, and other public and private databases. Markov, along with a team of hackers, targeted "Estonian essential infrastructures, telecommunications, name servers, web sites, e-mail, [and] DNS" (Colatin, 2007). Note the similarity between this case and the 2022 Russian targeting of Ukrainian central systems using a trojan malware (a kill disk malware that erases data) called, HermeticWiper that preceded the Russian invasion of Ukraine on the morning of February 24, 2022 (Symantec, 2022). Similar attacks were noted on systems in Lithuania and other Eastern European countries considered by Russia to be her near-abroad.

The attack on Estonian cyber systems was allegedly conducted in retaliation for relocating a Soviet statue commemorating the "Liberators of Estonia" from the capital, Tallinn, to a military cemetery on the city limits. While some view the statue as a Russian triumph over Nazi occupation, others see it as an insult to Estonian independence from the Soviet Union. Inflamed, the Russian Foreign Minister, Sergei Lavrov, made an ambiguous threat about "taking serious steps," resulting in widespread DDoS (distributed denial-of-service) attacks causing " email servers

mainframes failures, DNS servers overloading, and damaging of routers…" (Ottis, 2007; Prakash et al, 2016). Although neither physical damage nor full-scale cyber warfare ensued, the incident shook the entire nation.

However, despite the breach, internet voting took root, and positive outcomes unfolded alongside the drama in Estonia. Relative to its Finnish neighbors, Estonia has increased nationwide voter turnout. It also reduced the time needed to cast one's vote from 44 minutes (at the polling station) to 6 minutes (online). E-voting initiatives also significantly corresponded with increased women's participation in voting (Kalvet et al., 2013). Whether or not these advancements would have been sought after or achieved if the country had foreseen such an attack is unknown. However, it appears that once Estonia turned down this road, they could not go back. Balancing national security with advancements in administrative efficacy presents Estonia with a sink-or-swim security scenario that drove them to seek cyber-security collaboration with NATO. Soon, Estonia gained a reputation as "the most wired country in Europe" (Davis, 2007)

Estonian developers, aided by supranational partners, worked tirelessly to classify and address inherent risks. These included (but were not limited to) discrimination errors (otherwise known as "selective operability"), vulnerable internet connection (or intercepted via webpage mimicry directing voter to false page), web server/VFS (data accuracy of the virtual file system), the voter's browser selection, intranet (the integrity of private network or firewall), VSS (voting system standards), VCA (vote counting application), troubleshooting the 'validity confirmation service,' and creating a sturdy auditing system (Anspur et al., 2010). The security breach of 2007 was a double-edged sword.

On the one hand, it highlighted the devastating consequences of what could

happen if foreign entities exploited vulnerabilities in centralized cyber-infrastructure. On the other hand, it also sparked intense hyper-fortification, national collaboration with supranational entities, and sped technological advancement in cybersecurity worldwide. Due to the breach, Estonia possesses a far more securitized system than one might expect.

Estonia adopted blockchain-based e-voting infrastructure in 2012 when crypto platforms were in their most nascent form. Contextualized further, this happened just seven years after Estonia implemented e-voting technology (internet, not blockchain based), five years after the Russian breach, and two years after the ENEC security report was published. After supranational reinforcement, the system became so streamlined that even Barack Obama, tongue in cheek, once quipped, "I should have called the Estonians when we were setting up our health care website" (Martinson, 2019).

4.2 Exonum: Moscow city council elections (2019 and 2020)

The Moscow City Council Elections of 2019 present a curious case study, the first blockchain-based e-voting election ever conducted in Russia. For starters, it was openly acknowledged as an experimental initiative. The winner would be elected as a deputy for the Moscow City Duma. To launch the project, a technical team, with the oversight of Pierre Gaudry, an international law expert, began building a beta model to accommodate three voting districts participating in the city council elections.

While all other countries experimented with blockchain-based e-voting systems marketed in a politically wholesome way, Russia made no efforts to disguise it as purely experimental. This honesty sets it apart from other cases. Second, Russia's notoriety for hacking (see the Estonian case above), if wielded productively,

would be a sincere asset to fortifying. The study of cybersecurity itself is often referred to as "ethical hacking" — i.e., an attempt to crack your own system before someone else does. (However, we'll come to why I say 'would be' rather than 'will be' soon, but there is a glaring reason why blockchain-based voting may be doomed in this political context). Even so, looking at the experiment, we see many significant hurdles successfully cleared, from internal audits (predominantly led by Positive Technologies and Kaspersky Lab) to system testing (e.g., DDoS attacks, internet outages, blackouts, and other technical issues). (Polyakov, 2020). Though many milestones in the Moscow City Council Elections of 2019 deserve applause, some significant concerns remained unaddressed. For example, when vulnerabilities were first pointed out in the system, there were resolved. When, after revision, other issues persisted, they were let slide. It's possible that fixing them may have been beyond the relevant timeline of the experiment (i.e., if they intended to change or re-do the system so significantly, it would be a waste to invest time in the 'old version'). It's also plausible that their attempts to troubleshoot these issues were simply unsuccessful due to the limits of the version of Ethereum-available in 2019. Originally, ETH 2.0 (also known as "Serenity" was intended for release in 2019 but was delayed until June 2022 (McQuaid, 2022). It may have been far more suitable for this purpose than the ETH 1.0, the only viable version on the market at that time. In either case, the overall project was widely seen as a success. These experiments preceded significant changes to the Russian constitution (State Duma Bill No. 1065710-7 and Federal Law No. 259-FZ). Though the amendments of the Russian constitution were primarily designed for taxation purposes, they nonetheless facilitated an increasingly crypto and blockchain-friendly legislative environment in Russia (Frost, 2021). A more controversial amendment to the Russian constitution

was announced and submitted as a draft in January 2020, which created waves:

> "The entire Russian government is abruptly resigning to make way for Russian President Vladimir Putin's proposed changes to the constitution, Prime Minister Dmitry Medvedev said in an announcement on state television on Wednesday" (Klebnikov, 2020).

Medvedev resigned after Putin's annual address. A matter of hours after his resignation was complete, Putin announced that he'd selected a new prime minister: Mikhail Mushutin, head of the Russian tax service. It coincided with a broad set of legal revisions to seemingly unrelated issues — from exchanging the four-term limit for presidential leadership for six to reinforcing bans on same-sex marriage. Putin also shuffled Medvedev's role to deputy head of the Russian Security Council. Thus, the amendment was a catch-all for all legal splinters Putin wanted to sand down. Only one caveat was blockchain-related. It granted eligible Russian citizens the opportunity to use the blockchain-based e-voting system to vote on the amendments above. However, because amendments can only be voted on as a package rather than individually, "many critics accused the government of creating a 'Trojan horse,' hiding some arguably unlawful proposals among the legit ones" (Klebnikov, 2020). Thus, Russia's legal inclusion and support for blockchain-based e-voting infrastructure are likely to be benevolent or purposed for actual corruption reduction. That these constitutional revisions occurred amid a global pandemic further smoothed the way for drastic legal changes. In tandem with the increasing demand for remote options, this accelerated investment in blockchain-based e-voting systems as well. By mid-2020, a new system was released. As the endeavor scaled to accommodate more voters, the consequences of flaws in the system intensified. The day the new platform launched in Moscow and Nizhny Novgorod, it crashed. Eager

to use the new and improved system, voters flooded the platform as soon as it opened. According to Anton Lopatin, a member of the Central Election Commission: "The web portal for the remote voting on constitutional amendments crashed due to peak load" (Novosti, 2020). Though the system was restored in under two hours, allegations were made that much of this data was already sold.

In an expert column penned by Kirill Polyakov, head of the distributed registry technology department at the IT department for the city of Moscow who participated in the development process, he further discusses the internal complexities and competition of producing the project:

> "The technical working group included critical IT professionals, with the new members who became part of the group in 2020. For example, representatives of the Party Of Direct Democracy, which is a competitor, since its agenda includes the development of its own electronic voting. However, this is the case when joint participation in such projects strengthens and enriches each of the parties" (Polyakov, 2020).

There is a significant emphasis on international cooperation throughout Polyakov's writings and other literature on Russian experiments with blockchain-based e-voting. Though Pierrick Gaudry's declined to "participate in the audit of the [2020] system," his insightful comments on encryption mechanisms were widely praised by the Russian team. Moreover, Gaudry's primary reason for ending his involvement was "… due to the lack of documentation for the system in English" (Polyakov, 2020). No other information was provided. Professionals on the project are openly active on open-source platforms such as Habr (a Russian blog bringing together IT, Computer science, and TechMedia professionals) and GitHub (a global software development platform), among others. Thus, though flawed, the Russian parliamentary elections accommodated its largest scale of voters yet (nearly 30,000). (Note: the most

extensive system at the time was still held by Estonia, scaled to accommodate 270,000+ voters). The Russian case is fascinating because reviewing technical, political, and legal accounts of the blockchain e-voting experiment are wildly different in tone. The technical experts are enthusiastic about the progress made — irrespective of other implications. The political statements treat technological developments as an asset for agendas (namely, power consolidation and marketability) that fundamentally undermine the decentralized nature of distributed ledger technology (DLT). In contrast, the legal lens looks at blockchain-based e-voting systems as an earmark —worked in alongside countless other issues. Legal infrastructure mirrors political need— not technical demand. Sometimes their objectives line up; sometimes, they do not. Thus, Russian support for blockchain-based e-voting should not necessarily be heralded as a "safe" for scale despite the legitimate advancements made.

So far, the two case studies mentioned (KSI and Exonum) were created with the express purpose of vote tabulation. But suppose we broaden our scope to include other blockchain-based data management systems that also went into effect in approximately the same time frame that include*s* tabulation but which do not solely exist for these purposes. The Joint Research Centre (JRC) of the European Commission (in joint analysis with the EU Blockchain Observatory Forum) researched seven pilot projects deployed around Europe. Each use-case case study pertained to the distribution of public services and administration. The join-study assesses blockchain's various public administration implementations (including but not limited to electoral use-cases) in Georgia, Malta, Sweden, Switzerland, Luxembourg, and The Netherlands.

Table 3. List of Blockchain Projects (Non-Exhaustive)

Project No	Project Name	Country of implementation	Field of implementation	Level of government involved
1	Exonum land title registry	Georgia	Land title registry; property transactions	National
2	Blockcerts academic credentials	Malta	Academic certificates verification; personal documents storage and sharing	National
3	Chromaway property transactions	Sweden	Property transactions; transfer of land titles	National
4	uPort decentralised identity	Switzerland	Digital identity for proof of residency, eVoting, payments for bike rental and parking	Local (Municipality of Zug)
5	Infrachain governance framework	Luxemburg	Blockchain governance	National
6	Pension infrastructure	The Netherlands	Pension system management	National
7	Stadjerspas smart vouchers	The Netherlands	Benefit management for low-income residents	Local (Municipality of Groningen)

Source: [Alessie et al., 2019]

Per the European cases, there was also e-voting in Ireland. However, the pilot project fizzled due to declines in e-voting turnout and lack of a reliable auditing system. Thus, the most representative and relevant case for this manuscript is, arguably, the municipal elections of Zug, Switzerland (2018), featuring the uPort platform.

4.3 ETH + uPort: municipal elections of Zug, Switzerland (2018)

Situated in the tiniest of the Swiss cantons just south of Zürich in central Switzerland, the town of Zug is home to about 30,000 citizens. Renowned as a well-known tax haven, the Zug municipality is also known as The Crypto Valley. (Notice I said “the” not “a”). Though crypto ecosystems have proliferated around the world, this municipality was so conducive to initial coin offerings (ICOs) that Zug effectively became a global headquarters. Crypto entrepreneurs of the region then collaborated and adopted the name Crypto Valley Association, continuing their enterprise with the strong support of the Swiss government. They proudly claim to be

"the largest blockchain and distributed ledger ecosystem worldwide, based out Switzerland, with presence in entire Europe and beyond" (Crypto Valley Association, 2022). Where Switzerland differed in their experimentation is that they did not test the tech "real-time" in an actual election. Instead, they created a test topic with voluntary participants.

> "The trial involves citizens putting their voices forward in a consultative vote—Switzerland has a lot of those—on an invented issue. Zug citizens got to vote via smartphone, using the town's new electronic ID system" (Meyer, 2018).

Though its success was widely celebrated, turnout was considerably lower (understandable because the topic was fabricated). However, for the same reason, the low-stakes nature of the vote decreased the likelihood of cyberattacks — meaning that we should still be skeptical about over-confidence in security systems. Though it's clear that the success doesn't spell the end of the race, what makes the case interesting is that the capacity to vote (in an electoral context) was not the central focus of the pilot project. Rather, the crux of the project was decentralized identity. Though the use case of the uPort (a derivative of the Ethereum blockchain) was voting, significantly more focus was dedicated to the concept of using the chain to launch a government-issued identity. Here's what it encompasses:

Table 4. Resume of Government-issued Identity via uPort

Government-attested decentralised identity in Switzerland

1. General features

Level of government involved	Public services provided/enabled	Cross-border aspects	Cross-sector aspects	Location value creation	Openness of software
Local	Proof of residency	None	Yes	Location is static	Open source

2. Functionalities

Institutions disintermediated	Functionalities provided
None	Provenance (notarization)

3. Governance

Roles included	Blockchain governance architecture	Consortium governance
Government; OS community; tech provider	Public permissionless	Hybrid – various consortium partners

4. Usage

Current Usage	Capacity	Throughput	Scalability	Maturity
About 300 people	30k	Unknown	7 tps	Early stage pilot

5. Technical architecture

User Layer	Non-DLT Systems	API Layer	DLT Platform Layer	Infrastructure layer
uPort (mobile app)	Front-end portal	uPort Connect API	Proof-of-Stake consensus	Ethereum blockchain. User data stored locally.

6. Costs

Non-recurring costs	Recurring costs
Integration and installation cost	Transaction costs; operation cost

7. Benefits

Quantitative benefits	Qualitative benefits
Lower administration cost; lower storage cost	E-identity without a central administrator; citizen's control over data

Source: [Alessie et al., 2019]

Certified in November of 2017, the pilot phase commenced with six months of testing. Essentially, uPort is a consortium blockchain which means that it operates on a hybrid basis — a combination of public and private structural elements. Among the key contributors and administrators are: ConsenSys, TI&M AG, Institute of Financial Services Zug (IFZ) at the Lucerne University of Economics, and the City of Zug (Alessie et al., 2019). Though securitizing election tabulation was a part of the agenda, the principal focus was to find an alternative for identity confirmation and personal data management. Previously, such systems involving digital identity engaged with proof of residency. According to the EU joint research center (JRC), "The project however aims to expand to other public services run by the local authorities, like: surveys, e-voting, bike renting, book borrowing, tax declarations or parking payments" Alessie et al., 2019. To bring it to fruition requires citizens to first register with uPort. Effectively, this is a smart contract on Ethereum that is

guaranteed and administered by the Zug municipality (who maintains authority over the admin rights of the uPort application). Though the citizen must be physically present to verify their identity, following approval and a municipality attestation signed via private key, the individual is allocated a private key themself. This private key is a server-side credential (uPort ID), meaning that it is unique to the user to initiate an information transaction (e.g., a vote or some change of their personal data), but does not give them any visibility over other activities. In this way, it deviates significantly from fin-tech applications of blockchain, wherein any party can imitate (send) a data transaction (in this case, monetary value is the data transacted). This server-side credential (the uPort ID) is recognized as a government-issued identity. Below is a visualization of the citizen registration process (Alessie et al., (2019).

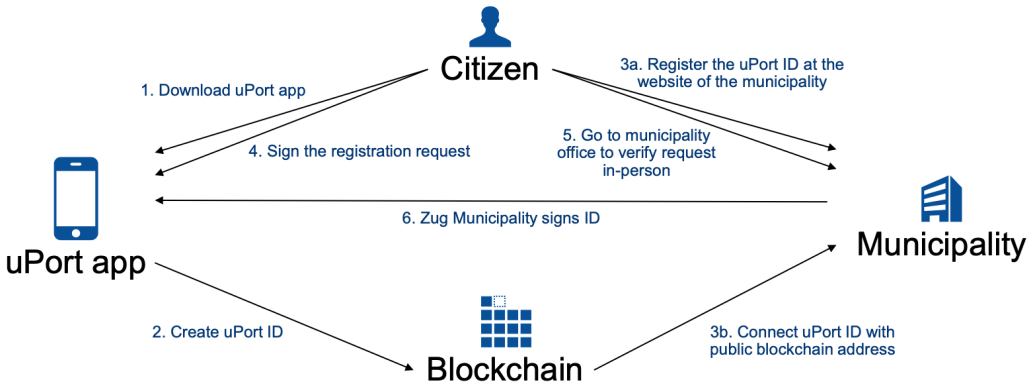

Figure 10. The uPort process overview
Source: [Alessie et al., 2019]

Each step is secured cryptographically, including the citizen signature of the registration (step 4) and the Zug municipality signature approving the ID (step 6). This personal data management system includes not just name and proof of residency but also current national ID number (existing prior to the uPort system), date of birth,

and can be modified to include other information. In recent years, the platform has expanded to include even bike rentals. However, at the time (2018), the pilot project took place on a parallel platform called a "Testnet" via Ethereum Rinkby. This became a fork of the Ethereum (ETH) main-net— i.e., not the core Ethereum chain (AnyBlock, 2020). The biggest difference between the two chains is that the former is scale. The Testnet pilot allowed 15 registrations per second and was limited in the number of participants it could accommodate (Alessie et al., 2019). When we look at a newer beta project (Hyperleger, for example, that accommodates limited participants and can keep the tempo with 20,000 transactions per second), Testnet looks glacially slow (Gonzales, 2022). Though only a few hundred Zug residents opted into the pilot project, they likely wouldn't have noticed anything drastically different in their interactions with this (decentralized) app versus other (centralized) apps. Although their participation contributes to a major and unprecedented infrastructural change in personal data management, it's unlikely that they would notice anything beyond the convenience factor.

Whether this is efficiency at its finest or the precursor to a very Orwellian dynamic is yet to be seen. However, what makes the uPort registry unique relative to previous personal data management systems is its layered verification technique. For instance, if we were to reframe the steps figure illustrated above, we might conceptualize the transaction flow like this (uPort Developer, 2022).

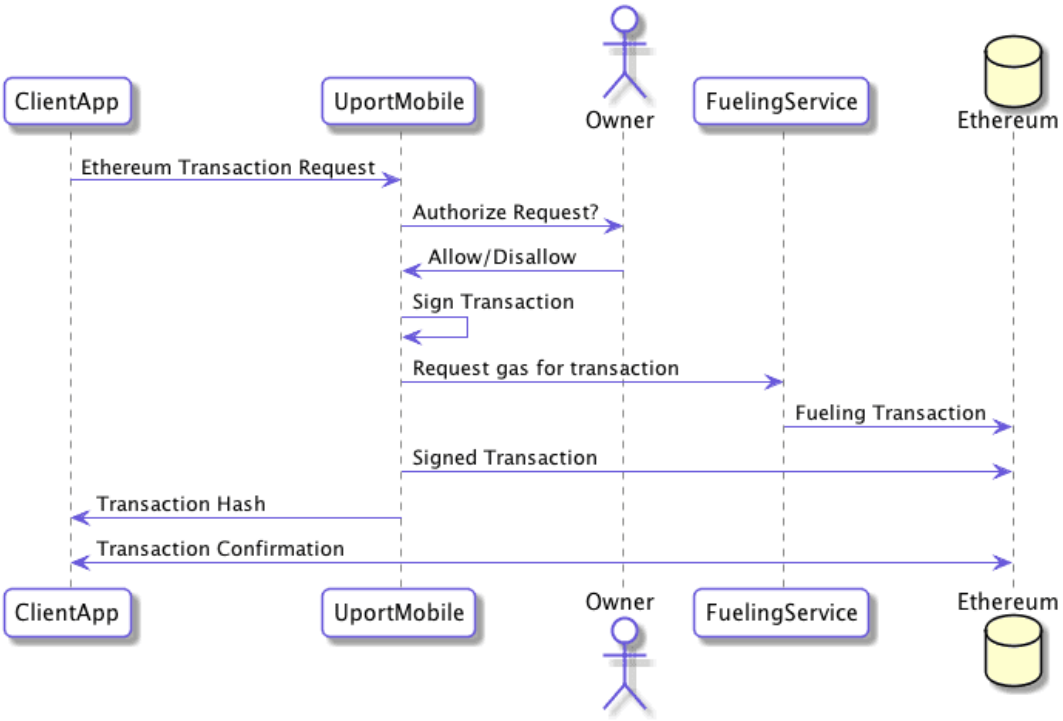

Figure 11. Basic uPort transaction flow
Source: [uPort Developer, 2022]

This chart (though perhaps more complex at first glance) allows us to see more finely where smart contracts fit in the technical architecture of the uPort project. Smart contracts are the most critical part of the uPort registry service. Every user registered on the system engages with two forms of smart contract known as (1) a “controller” and (2) a ”proxy” or identity contract. The first acts as an authoritative entity — granting or pulling back authorization to be a signatory on statements. The second (the identity contract) is the public “face” of the user identity. Though the proxy is considered a “sovereign entity” that can interact with other smart contracts on the uPort platform, none of these interactions are centralized (Alessia et al., 2019). Instead, the controller smart contract (#1) monitors the proxy contract (#2). This is a standard infrastructural component called “IPFS” or InterPlanetary FileSystem, built in 2015 to overcome the security inadequacies posed by the client-server dynamic of

HTTP (HyperText Transfer Protocol) invented in 1991.

The name IPFS is descriptive of its verification dynamic: it is an aggregate of peer-to-peer (P2P) protocols articulating data movement within a network. The term 'interplanetary' reflects the many protocols existing in the same digital space. According to Kwantra, "with HTTP you are asking what is at a certain location whereas with IPFS you are asking where a certain file *is*" (Kwantra, 2018). The former uses targeted location; the latter is proximity oriented as well. According to Juan Benet (the inventor of IPFS, CEO of Protocol Labs, and founder of FileCoin) describes its functionality with respect to blockchain:

> "IPFS connects all these different blockchains in a way that's similar to how the web connects all these websites together. The same way that you can drop a link on one page that links to another page, you can drop a link in Ethereum [for example] that links to Zcash and IPFS can resolve all of that" (Benet et al., 2015).

IPFS doesn't require servers, meaning local users can communicate and interact despite network blocks. It is typically much faster due to better bandwidth. The system also relies on proximity (i.e., it is spatial and relative to what exists around it) rather than a linear path (an isolated coordinate). This fosters an entire data ecosystem into existence. The diagram below depicts how PoS logic and IPFS frame the entire uPort SmartContract platform (Kassem et al., 2019).

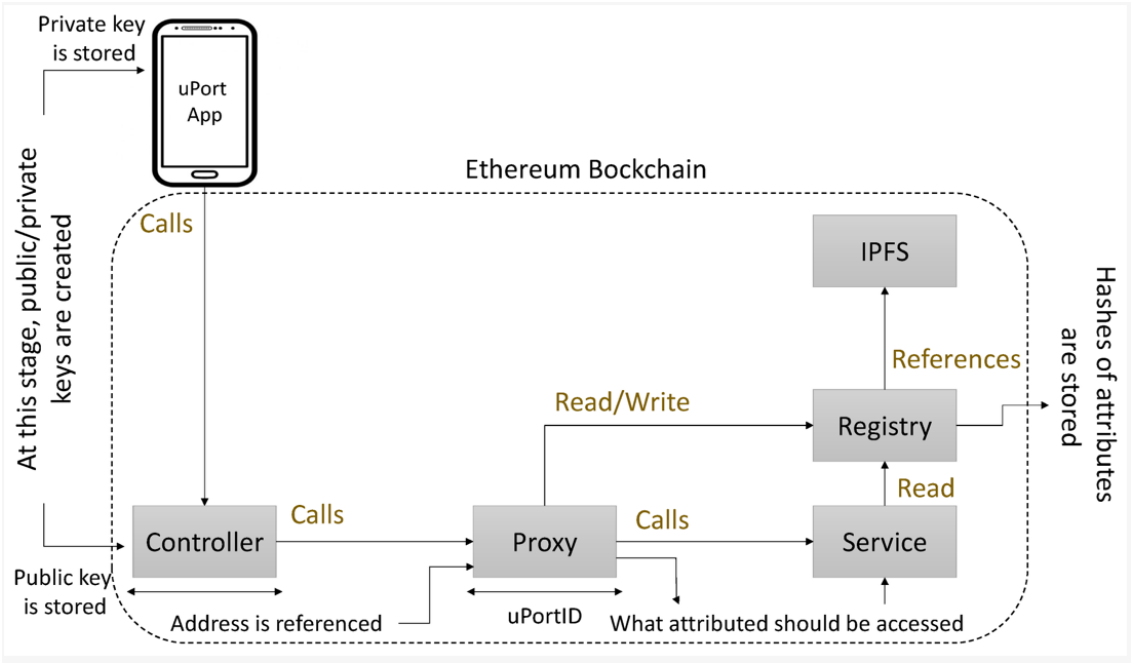

Figure 12. The general architecture of the uPort InterPlanetary FileSystem (IPFS) Source: [Kassem et al., 2019]

Thus, UPort platform itself is not a DLT, nor is the Zug municipal registry. The uPort platform and Zug municipality are localized, respectively, separate from the DLT. As we walk through the uPort workflow, recall that a blockchain is a type of distributed ledger tech, but not all DLTs are blockchains. Essentially, the DLT is a database administered and managed across multiple participants and nodes. A blockchain is a type of DLT that relies on a hash (an immutable cryptographic signature that is the product of converting data into an indecipherable text string) to record each transaction (Hackernoon, 2022). Note that any given DEX (decentralized exchanges) lives on top of a blockchain. It is typically financial. What we're concerned with here are DLTs and blockchains, not DEXs. To make any progress in the analysis, we must shed our biases in synonymizing DEXs with DLTs.

So, when we look at Figure 11., we might not notice that uPort exists as an intermediary corridor between the owner (Zug municipality) and the Client dApp (decentralized app). However, shifting our gaze to Figure 12., we notice that the

entire Figure 11 graph fits on the line connecting the uPort App to the Controller.

Rather these are autonomous, external, and heavily fortified databases anchored to ETH via SmartContract (digital contracts that automatically execute task sequences according to scripted pre-conditions identified in the software program). Moreover, attestations are initiated off-chain and verified on-chain. This reduces the propensity for mass manipulation and data vulnerability in all phases.

What's happening in the rest of Figure 12? A front-end web portal connects the user identity (via their smart contract address) from their device with their resident number (associated with the municipality). (Note: this front-end web portal is likely the inspiration behind the name "uPort)." This coupled identifier is then translated to a QR code, allowing all sensitive information (name, DOB, ID, citizenship status, etc.) to remain localized— external to the DLT. It is this QR code that engages with the DLT blockchain. The user only engages with the platform via the uPort app through their private key (client-side credential), and their information lives in the system via the public key (the server-side credential). Thus, the uPort system decentralizes the user's identity. Since this is the priority focus, the use case can then be adapted far more malleably than if the target was one element of public administration (tabulation, in the case of this manuscript). This is arguably the strongest example worldwide of how blockchain technology might be safely implemented to improve not simply elections but other genres of public administration. Bravo, Switzerland.

4.4 xID + UniLayerX: Tsukuba, Japan (2018)

Tsukuba is to Japan as Zug as the Crypto Valley is to Switzerland. Located in the Ibaraki Prefecture, the city of Tsukuba is well known for being a scientific hub (Jiji, 2018). So, it is no surprise that this was the first city to integrate progressive tech into

public administration affairs. More recently, the city of Kaga also began offering a blockchain-based e-voting option to its citizens in the same manner as Tsukuba (Cointelegraph, 2020). However, at the time, Tsukuba was a standalone first in Japan. On behalf of the Tsukuba city council, one spokesperson declared:

> "We are aiming to realize a 'Tsukuba Smart City' that is formed by linking technology and measures that correspond to it. We expect that the council's efforts will be accelerated by the participation of LayerX" (Ledger Insights, 2020).

LayerX (UniLayerX) is a Tokyo-based, De-Fi champion blockchain built on top of Uniswap (UNI), a New York-based application. UniSwap itself is built on the Ethereum (ETH) network— and is headquartered in Zug, Switzerland (CBInsights, 2022). Uniswap's original functionality was structured as a decentralized exchange (DEX) that allowed different tokens to be exchanged as long as they were built on ETH. Now, Uniswap v3 allows for non-fungible tokens (NFTs) trading. In terms of trading volume, Uniswap is one of the largest exchanges. Much of this is attributed to the developers' priority to increase the liquidity and reduce gas fees (transaction/commission fees paid by users to cover operating costs—like the computer energy needed to process and validate ETH transactions) (Frankenfield and Rasure, 2021).

> "Unlike other decentralised exchanges, UNI tokens allow holders to trade in any two ETH-based crypto coins, which is termed as a 'swap.' The action is seen as a more liquid way of exchanging large amounts of crypto…UNI traders can purchase, sell and hold the crypto tokens via credit cards, debit cards, bank transfers as well as digital wallets – providing fluidity in trading gateways. The exchanges can be facilitated via trusted crypto exchange platforms that allow UNI purchases with competitive fees and low spreads" (Parashar, 2021).

Japan's LayerX and Switzerland's uPort projects were implemented at roughly the same time (2018). Both platforms relied on a similar smart contract system to the uPort design described in the previous case. In addition, they used a permissioned chain for personal data management and anchored it to a public, permissionless chain to run the system. The biggest difference is that the chain used by Japan uses Uniswap to bridge the information exchange — making it one level distant from the anchor chain (ETH). (Speculatively, this probably reduces fees). Although the Uniswap V2 (version 2) has been updated to V3, the automated liquidity protocol retains similar logic (Uniswap Platform Docs, 2022).

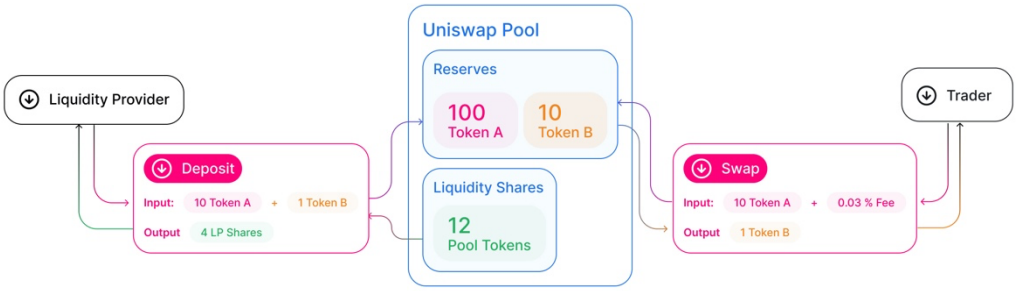

Figure 13. Uniswap V2 automated liquidity protocol
Source: [Uniswap Platform Docs, 2022]

This is one of the core functions that make Uniswap unique as a DEX. When LayerX (UniLayer) was built atop Uniswap, it was among the trailblazers of the 2018 De-Fi (decentralized finance) boom— another wing of the movement seeking to streamline transactions by eliminating financial intermediaries through DLT. UniLayer's core focus was "flash utility," which alludes to removing barriers to use and liquidity (Uniswap platform docs, 2022). Furthermore, UniLayer (LayerX), headquartered in Japan, offered "professional-level trading with its LAYER utility token, focusing on automated swaps and liquidity management, flash staking, charts and analytics, live

order books, and more" (Messari, 2022). So, LayerX is a digital asset token living in an ecosystem (UniLayer) built on top of an exchange (Uniswap) anchored to a network (Ethereum). Thus, the Ibaraki Prefecture (home to the city of Tsukuba) partnered with LayerX — headquartered in Tokyo— to build a citizen registry (xID) anchored to the LayerX ecosystem. From here, the xID uses Smart Contracts in— more or less— the same way as uPort in the Swiss case. It's no small irony that the nickname of UniLayer is the "Swiss Army Knife of DeFi." Though the name alludes to its usability and versatility, it's system design bears remarkable resemblances to the Swiss uPort platform.

4.5 Voatz pilot project (2018), municipal (2019), and federal (2020) elections

Perhaps the most worrying case study of blockchain-based e-voting systems in this analysis is Voatz, the Boston start-up that runs on Hyperleger. What's concerning about it is that it looks and feels a lot like the other initiatives we've discussed so far to the untrained eye. It was implemented as a pilot project around time (2018) as other global case studies, and it was done on a similarly petite scale with fewer than 600 voters per pilot project (Amicus brief, 2020). The first of these live-action pilot project votes was tested on a small crop of overseas military voters in the 2018 West Virginia Primary (Miller, 2020; Weiss, 2019). This is unsurprising as the military presents a ready and compliant population for scaled testing of all genres because they have no freedom to abstain. In addition, tabulating deployed military votes has forever presented a logistic problem so there's tangible motivation to resolve this issue. One year later, Voatz also became a voting option for municipal elections held in the city of Denver (2019) and five countries across West Virginia, Utah, Colorado, and Washington State (Lee, 2020). Following Voatz's experimental involvement in

these elections, the National Cybersecurity Center (NCC) conducted an audit that viewed the platform as a success (NCC, 2019). In 2020, the platform then became the first-ever blockchain-based e-voting system to be used in the U.S. Federal Elections. Voatz has even won numerous awards attesting to its credibility.

Yet, despite the similarities in timing, rhetoric, dispersion, and public praise, it bears significant structural differences from any of the previous cases described. Rather than using a permission chain anchored to a public chain, Voatz uses a private, modular, enterprise-grade blockchain leger anchored to a consortium/hybrid chain. Voatz was built atop Amazon's AWS and Microsoft Azure, and these are then powered amongst 32 identical nodes powered by Hyperleger Fabric (HF) and a private offshoot of Hyperleger. Essentially, Voatz is a private, mobile application that attempted to use blockchain to do what each case thus far has attempted: create a more secure, more efficient means of voting. In terms of rhetoric, Voatz acknowledges many (if not all) of the issues outlined within chapters one, two, and three of this manuscript.

Where it deviates entirely is that this platform was reverse-engineered from an Android app. The model almost implies that they sought to tailor the problem to their desired answer, rather than looking at the problem and crafting a solution designed to satisfy the umbrella necessity this issue highlights: personal data management. Moreover, it was designed without the explicit expertise of cybersecurity and other security professionals. In other words, this is a complete repeat of the original problem we saw in EVM production. Private producers saw an opportunity to make a product that would satisfy the goal of counting while taking insufficient steps towards security. This is perhaps the most dangerous mindset to transfer into blockchain development. The result has been a system is vulnerable to

side attacks, has not provided adequate transparency, and relies upon more biometric measures than any of the systems discussed thus far — even Russia's Exonum. Despite demanding more sensitive biometric information, they've released very little information on whether this is localized (as in the Swiss case) or how the system is securitized. Voatz is significantly *less* transparent than all other chains analyzed thus far, including the Estonian chain, which was redesigned after its most significant breach with heavy oversight from the U.S. Department of Defense (whose eyes peer through NATO). As we try to unravel the general system architecture of the Voatz platform, we can adopt a client-side or server-side perspective. The user (client-side perspective) flows through a process that feels like this (Specter et al., 2021).

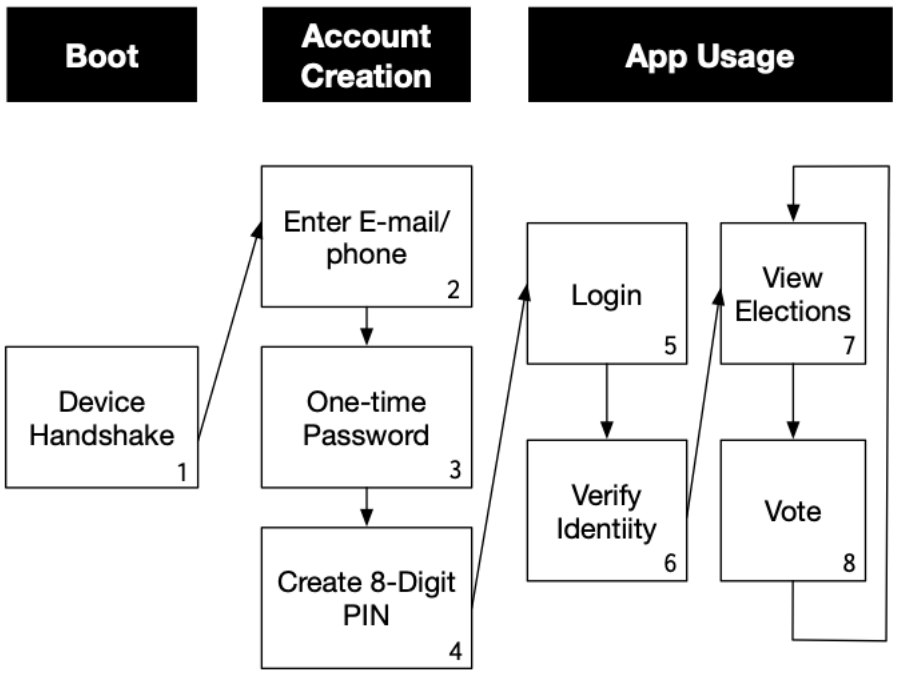

Figure 14. Voatz workflow as seen from device (user perspective)
Source: [Specter et al., 2021]

It's extremely user-friendly because it resembles other client-server models the general public has been conditioned to use since the 1990s. First, however, here's

what's happening behind the scenes (the client-side perspective) (Specter, Koppel, and Weitzner, 2021).

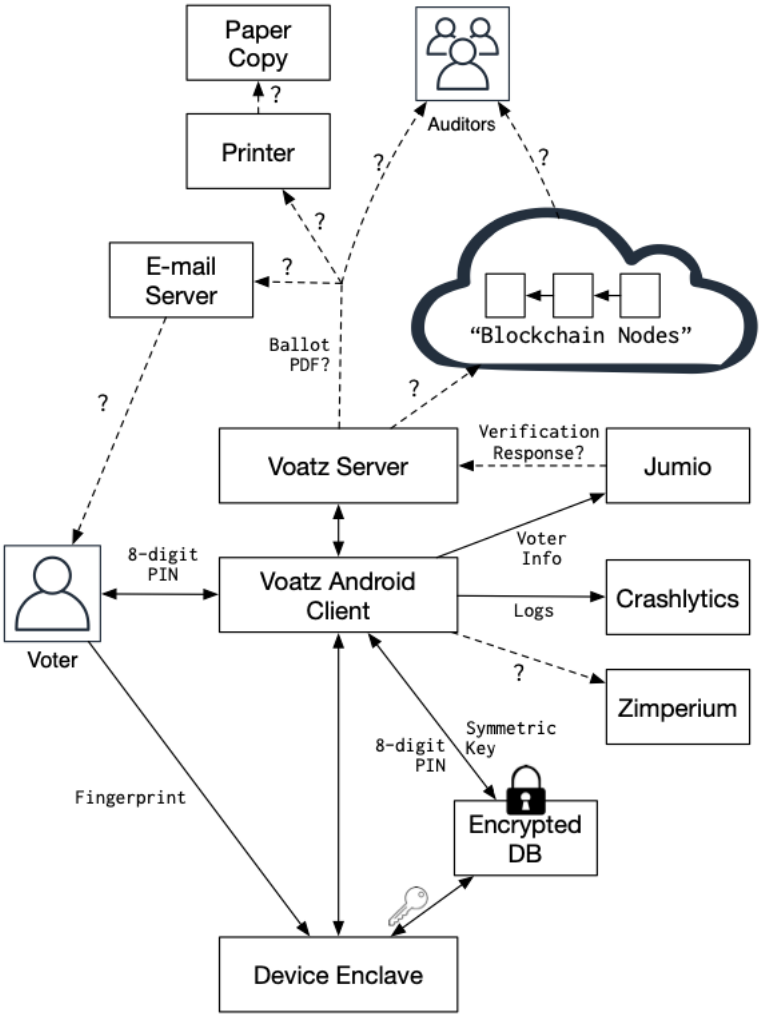

Figure 15. Data flow between Voatz components and external services
Source: [Specter, Koppel, and Weitzner, 2021]

According to Specter et al. of MIT, the "dashed lines are believed to exist but have not been directly observed" (Specter et al., 2021). Likewise, they note that "Voatz has presented no formal threat model and has failed to release a full description of their system (Specter et al., 2021). This is consistent with claims from other security analysts such as Schneier, who noted "no public description of the security model" (Schneier, 2021). (Note: you might remember Schneier as one of the most outspoken

analysts alerting the fatal flaws of WinVote AVS in the early 2000s). The only breadcrumbs we notice of Voatz addressing security claims is in an FAQ which, while descriptive, may be nothing more than words. The proof is in the pudding. With these uncertainties in mind, the aforementioned research team at MIT conducted a thorough security analysis and internal audit of the system design (Lee, 2020). After a series of layered authentication steps and verifications, the vote is submitted through an API server first— not directly to the blockchain. Moreover,

> "….although the user is asked to authenticate before submission, beyond the MAC associated with the AES-GCM algorithm and enclosing TLS session, the text of the vote itself is not otherwise signed. The only indication of blockchain-like tokens being submitted or exchanged is the 'auditToken,' but this string is never altered by the app, and appears to be a single, static value" (Specter et al., 2021).

They discovered this by testing a synthetic (fake) election and by decrypting the payload of a hypothetical voter. In their experiment, this 'voter' was a black cat whose facial recognition was registered with an identifying scrap of paper reading, "This is a passport. Also, I am a cat." Through a number of auditing techniques tracking the cat's voter data, the team created a "Summary of Potential Attacks."

Table 5. Summary of Potential Attacks

Adversary	**Attacker Capability**				
	Suppress Ballot	Learn Secret Vote	Alter Ballot	Learn User's Identity	Learn User IP
Passive Network (§5.3)		✓			✓
Active Network (§5.3)	✓	✓			✓
3rd-Party ID Svc. (§5.4)	✓			✓	✓
Root On-Device (§5.1)	✓	✓	✓	✓	✓
Voatz API Server (§5.2)	✓	✓	✓	✓	✓

Source: [Specter et al., 2021]

Thus, the Voatz API Server (where personal voter data passes through before being stored on the chain) is susceptible to each of the five means of manipulation tested. In other words, it may not matter how immutable and secure the blockchain is if the information is vulnerable just before it is encrypted into the chain. Despite the thoroughness with which the analysis was conducted, there were evident flaws made clear by the Voatz once they read and responded to the report. Among them, the version analyzed was (at that time) 27 versions old, meaning that 27 upgrades had occurred since the initial analysis. These improvements have likely increased, and certain issues identified in the document may have already been addressed by the time of the analysts' publication. Second, they noted that direct engagement via Microsoft Azure and AWS did not occur. However, a looming counterargument to this rebuff would be that the expiration of Azure was imminent, even at the time this statement was issued. Since the time of these publications (the security analysis and the response in 2022), Microsoft Azure retired in January 2022 (Azure Scheduler, 2022; Protos, 2021). In the view of Voatz, because the researchers could not access the servers, they had no right to extrapolate as to how these users engage with the system infrastructure. While this could be viewed as a symptom of lacking transparency in itself, Voatz instead replied with emotion first, empires second. The opening line of their response to the MIT security article cited above is this:

> "Voatz wishes to acknowledge the enormous effort it must have taken for the team of researchers, until this point anonymous to us, to produce 'The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S Federal Elections' (Voatz Response, 2020).

To address a security concern with a sardonic jab is unprofessional at best and dangerous at worst. The role of the security analyst is to seek out vulnerability so that

infrastructure can be improved and users can be protected. If it is unsound, this is not the problem of the analysts but the system architects. Yet, at one point in their Voatz response statement, they assert, "…with qualified collaborative researchers, we are very open…" (Voatz Response, 2020). This was followed up by a technical analysis that was condescending towards these concerns from its title onward: "A Brief Technical Analysis of Claims Made by Some Researchers from MIT" (Voatz, Inc., 2020). If anything, the title should have indicated which technical issues would be addressed, not highlighted a petty gripe with academicians. Yet, here we see the company try to diminish the status of the persons who raised concerns by casting them as 'just some' people. Their emotionally evocative reply to an empiric article bears all the hallmarks of gaslighting — it's-not-me-it's-you mentality. That Voatz interpreted the MIT analysis as a personal affront (rather than a welcome insight into how their system could be improved) is a serious red flag. In neither business nor security is immaturity ideal for progress, particularly when the opportunity costs are so high. Schneier drives straight to the point:

> "Voatz has a number of privacy issues stemming from their use of third party services for crucial app functionality…The company's response is a perfect illustration of why non-computer non-security companies have no idea what they're doing, and should not be trusted with any form of security" (Schneier, 2022).

Moreover, when a company gets inflamed over a lack of transparency — especially when it is a lucrative enterprise that has the potential to affect mass amounts of personal data — does that raise suspicions? Absolutely. Moreover, their response mirrors a distinctly American trend where it has somehow become normalized to dismantle and belittle an opponent's reputation and personal standing rather than

critique the technicalities of their stance. Anyone who gave up watching presidential debates or noticed the public slander of medical professionals for research findings contradicting pharmaceutical interests can recognize that these fall into a slew of common power plays eminent in the way America operates in the corporate and political realm. Though there are many positive signatures of American institutions, this emotionally-charged dominance-assertion tactic is not one of them. That Voatz presents so much less information to the public relative to the other cases reviewed in this manuscript (Estonia, Switzerland, Japan, and Russia), demands more biometric verification from users, and has shown poor dispute resolution management is highly concerning. In Voatz, I do not see an ideal platform for improving voting processes; I see a corporate bully in the making,

In previous publications, they wrote from a stance of superiority, annoyance, and condescension. As their PR spiraled, they attempted to refocus the dispute by presenting themselves as pioneers and reframing the researchers as malicious.

> "We are often the subject of doubt, and new technologies are frequently the target of skeptics. A group of researchers, in an effort to trigger a media campaign geared to systematically disrupt a live election process, contacted The New York Times with allegations of vulnerabilities in our system" (Voatz, 2020).

Following their initial inflammatory response to the two students and their supervisor, Voatz also reframed their points in a softer tone and published it on PR News Wire with less emotion and more substance (PRN, 2020).

> "We want to be clear that all nine of our governmental pilot elections conducted to date, involving less than 600 voters, have been conducted safely and securely with no reported issues" (Voatz, 2020).

None of the information in the News Wire differed in content, only tone. However, actions speak louder than words. Shortly after the above statement, they also expressed intent to expand their target demographic from predominantly deployed military voters to include the disabled and infirm (encompassing an additional several thousand voters) (Voatz Whitepaper, 2022). By 2021, it branched out to the Philippines (Regina, 2021). It also fundamentally failed to address the core concerns: the issue with Voatz was not that their platform *had been* hacked during these real-life pilot tests; it was that this platform was *highly vulnerable* to it.

Other statements peppered the documents released after the PR scuffle alluding to empowering overseas military men and women, disabled individuals, and expatriated citizens. Having lived most of my adult life as an expatriated citizen, I fall directly with the user demographic they claim to protect. Indeed, this bolstered a significant part of my interest in beginning this research, particularly when I was required to sign an affidavit surrendering my anonymity to participate in the 2020 elections from my foreign country of residence. I am, essentially, their target audience. Yet, I do not feel unjustified in my skepticism, nor would I ever align myself with individuals trying to disrupt a live election process as the company has repeatedly painted those harboring concerns about how they conduct their business. Despite the rhetoric lashing out at the students and their advisor, the Department of Homeland Security took the MIT researchers' claims seriously enough to arrange an investigation and set up briefings for municipal and state entities seeking to use the platform.

At the forefront of the arguments made against using Voatz has been their lack of transparency. No one outside the company knows how their securitization system works. This creates obstacles to verifying their claims are truthful and valid.

A New York Times article written by the Pulitzer Prize-winning author, Mathew Roseburg, raised similar concerns after being approached by the MIT researchers:

> "Beneath that criticism, there is also some very real animus — many in the tightly knit cybersecurity community blame Voatz for helping spur an F.B.I. investigation of a University of Michigan graduate student who tried to breach the company's systems in 2018. The student says he was conducting research" (Rosenburg, 2020).

Rosenburg directly addresses the MIT report mentioned above as well:

> "Flaws in the app, the report says, would let attackers monitor votes being cast — and might even allow them to change ballots or block them without users' knowledge. Perhaps the biggest risk, according to the researchers, is that the attacks could create a tainted paper trail, making a reliable audit impossible" (Rosenburg, 2020).

One of the key arguments used by Voatz is that it has used biometrics *to overcome* some of the issues posed (such as transparency, data vulnerability, and monopoly). However, is this cause for consolation or greater concern? The most immediate issue identified on the Voatz platform would be the vulnerability of the information on the system, perhaps even more than accuracy—if we were to triage. Asking users to provide more sensitive information is not necessarily a comfort if those vulnerability concerns are still present. That simply means that more of your data identity is out for grabs. Your biometric data makes your Social Security Number look comparatively less unimportant— and this is one of the most essential identifiers if an individual in the United States wants to integrate into the politico-social-financial system fully. You cannot complete any core function— from owning a valid birth certificate, holding a job, renting or buying a home, or, of course, voting— without having this number.

Your place in society is inextricably tied to this number. Biometric data will likely surpass this in terms of significance because it has the capacity to represent you internationally.

4.5.1 Monopoly

What further sets Voatz apart is not simply that it is a frontrunner platform. It is the *only* platform offering voter services in the United States at this time. Though Voatz shares the same anchor (HF) as several other major US-headquartered companies (such as PayPal, Mastercard, etc.), the Voatz platform differs significantly from these institutions. For one thing, none of these major corporations openly involve themselves in a federal governance institution in a core infrastructural way. Voatz's scope appears to be within the frame of creating a private (i.e., centralized) database for private corporate interest. Even in a standard corporate environment, all participants would voluntarily engage with these platforms based on trust, reputation, and perceived value offered over competitors. However, because Voatz is the *only* option available and it is seeking to claim the contract for internet-based voting platforms before any other exists, multiple concerns emerge: (1) monopoly de-incentivizes improvement, (2) this would privatize the entire nation's personal and biometric data, (3) that it has been built with corporate — rather than security— intentions has already left significant needs unmet.

Moreover, it's striking to note how much collaboration the United States Department of Defense has contributed via NATO to the successful fortification of the Estonian system but has been present predominantly in the form of audits of the system unfolding within its own borders. If this proves to be true, the United States will soon face an even greater data vulnerability crisis than what Snowden unearthed

in 2013 (Segal, 2017). I sincerely hope the above statement does not come to fruition. Though some might argue this is fear-mongering, it's also important to address the qualifications of those quick to dismiss these security concerns. For example, one Voatz investor, Bradley Tusk, who gained eminence as "an American business-man, venture capitalist, political strategist, writer and former campaign manager for Michael Bloomberg," has backed Voatz as a start-up and supported them amid this PR storm (Tusk Strategires, 2021). Tusk weighed in on the security concerns during an interview with the Havard Business Review:

> "It's not that cybersecurity people are bad people per se…It's that they are solving for one situation, and I am solving for another" (Tusk, 2019; Weiss and Haylard, 2019).

Though Tusk is an intelligent individual, is he the right individual to be dismissing cybersecurity specialists on a cybersecurity issue? No, his qualifications do *not* extend where his words have. Conflict of interest is only one problem with his dismissal of valid concerns. This is a scenario in which the blanket goal of 'increasing participation' over-emphasizes one metric of tabulation while ignoring other measures of success. We heard similar rhetoric in 2002, with the implementation of the Help America Vote Act (HAVA). The HAVA-hype helped entrench AVS WinVote, one of the most vulnerable systems ever entrusted:

> "Touchscreen voting machines used in numerous elections between 2002 and 2014 used 'abcde' and 'admin' as passwords and could easily have been hacked from the parking lot outside the polling place, according to a state report. The AVS WinVote machines, used in three presidential elections in Virginia, 'would get an F-minus' in security, according to a computer scientist at tech research group SRI International who had pushed for a

> formal inquiry by the state of Virginia for close to a decade" (Theilman, 2015).

Though well-intentioned in its endeavor to increase voter participation, the initiative accelerated the pre-mature adoption of nascent electronic systems—such as the AVS WinVote— which were riddled with vulnerabilities. In other words, if we strive *only* to increase participation, other cybersecurity concerns are at risk. When Voatz and respected public figures (such as Bradley Tusk) endorse any platform promoting participation without due diligence on security, they are driving history to repeat painful lessons. Will Voatz become the new WinVote? The 'next best thing' that is entirely different yet exactly the same? Pushing technological adoption for the sake of turnout alone is likely to yield positive results in improving scalability and speed. However, accuracy and anonymity stand to suffer significantly and at a much larger scope than before. This is the fear. Rushing to kickstart turnout without due diligence on other security concerns may simply mean that the fundamental problems of inaccuracy, data vulnerability, and manipulation might compound. In the words of Park, Specter, Narula, and Rivest (2021), we very well might be on the brink of "going from bad to worse."

> "Those who favor increasing turnout, reducing fraud, or combating disenfranchisement should oppose online voting because the possibility for serious failure undermines these goals. Increased turnout only matters in a system that meaningfully assures that votes are counted as cast. The increased potential for large-scale, hard-to-detect attacks against online voting systems means increased potential for undetected fraud, coercion, and sophisticated vote tampering or vote suppression targeting specific voter groups. What is more, online voting may not increase turnout" (Park et al., 2021).

This may be an extreme statement. However, they note that other studies in

Switzerland, Belgium, Canada, and Estonia, found either no significant increase in voter turnout after offering internet voting options or an increase that favored the upper-class with access to smartphones (Germann, 2017; Stewart, 2018; Goodman, Serdült, 2015; Pew Research Center, 2019). This stands in marked contrast to researchers studying these topics a decade before, in an era of optimism (for example, Gregorios, Spiraki, Nikolopoulos, 2010 or Wimmer, Scherer, and Appel, 2015). Please note, this is not to say that these researchers remained fixed in their position, but that the pieces published at this time reflected a certain degree of optimism in emerging technological infrastructure that is being received by increasing skepticism today.

To mitigate the PR disaster on their hands, Voatz wrote a supreme court briefing (an *amicus* brief) after trying to invoke the Computer Fraud and Abuse Act (*Amicus Curiae* No 19-783, 2020). Voatz adopts the stance that unauthorized security research could be interpreted as criminal and should be prosecuted as such. While the CFAA certainly has a place in modern digital culture, the researchers obtained what Voatz claims "excessive unauthorized access… [18 USC §1030(a)2)(C)]" is not, technically, out of legal bounds for them to complain about (Amicus Curiae No 19-783, 2020). However, it is at the crux of the cyber-security paradigm— often dubbed the field of ethical hacking. It's also that, more than the hack itself, the company was afraid of the publication — either for public relations purposes or a genuine fear that, if no hacks have been attempted, now ill-intentioned individuals might try. The pitted Voatz, as a corporate identity, and against academicians and rising professionals. Via the briefing, Voatz gave this official response:

> "…Further, as the researchers admitted, they were never able to get access to the Voatz servers using this outdated application. This meant that the researchers were unable to register as a legitimate voter, unable to test or pass

> the layers of identity checks required to verify a legitimate voter, unable to receive a legitimate ballot, and unable to submit any votes or change any voter data. Instead, the researchers fabricated an imagined version of the Voatz servers, hypothesized how they would likely work, and then made assumptions about the interactions between the system components that turned out to be false. In other words, by conducting their activities on an unauthorized basis rather than through Voatz authorized *bug bounty* program or direct collaboration with Voatz, the researchers rendered their own findings relatively useless" (Amicus Curiae No 19-783, 2020; emphasis added).

A "bug bounty" program is an open call arrangement wherein a company invites individuals ("friendly hackers") to identify and report bugs in their system. The scenario presents a win-win in that the company receives valuable input, and the hacker receives recognition and cash rewards. An insightful article on how recruitment of strutting these programs is titled "Given enough eyeballs, all bugs are shallow" (Maillart et al., 2017). The premise is this: if you look, you will find. Further, if enough people look ('enough eyeballs') or review the system, then problems ('bugs') in the software are more easily detected (shallow). Bug bounty programs are something of an all-call examination. Though bounties are common practice for tech giants like Facebook and Google, this strategy was met with understandable trepidation at the national governance level. The Pentagon didn't initiate their first bug bounty program until March 2016 (Greenberg, 2016). This correlates roughly with the decommissioning of the WinVote system (2002-December 2015) and with heightened concerns over Russian intervention in the 2016 U.S. Presidential elections. That these fears failed to subside moving through the 2020 election cycle plausibly played a role in the global realization that current tabulation systems— whether exploited or not— *are* vulnerable, and alternatives must be sought out. With the notable exception of Estonia, the bulk of blockchain-

based e-voting pilot systems were implemented for beta-testing in 2018. In the early chapter, we noted how institutional distrust manifests at the citizen level. This is infrastructural experiments amongst system architects might be read as another externality of distrust — or perhaps dissatisfaction— with the current systems available. (Whether positive or negative remains to be seen). Another trust-related shift is evident in the U.S. Government's adoption of the bug bounty programs described above:

> "The federal government, despite its massive IT spending, has seen repeated breaches over the last several years, including the unprecedented, disastrous breach of the Office of Personnel Management and a hack of the Pentagon itself last year---possibly by Russian hackers---that resulted in the shutdown of the Pentagon's unclassified email system for weeks. The bug bounty program represents a new approach to shoring up the Pentagon's defenses, and reflects Defense Secretary Carter's focus on Silicon Valley as a source of innovation that can be adapted to the military" (Greenberg, 2016' Kube and Miklaszewski, 2015; Alba, 2016; Hempel, 2015).

This strategic shift occurred during the tug-of-war with Apple during the San Bernardino case (see Chapter 2). During this time, Defense Secretary, Ashton Carter, prioritized visits to Silicon Valley with the same objective of building goodwill as one might do to bolster foreign relations. There is such a distinct canyon between the tech community and Washington D.C. that designated meetings intended to "rebuild bridges between the Department of Defense and some of our nation's most innovative industries" are needed to signal how far apart they've drifted rather than their inherent closeness (Department of Defense Briefing Transcript, 2016). Nonetheless, advancements in cyber warfare in tandem with cybersecurity have prompted both revisions of the bureaucratic and technological communities in an administrative context favoring corporate interests (Segal, 2017). Voatz engages with

the government and legal system as a corporate identity first — product over service. The dApp is their product; securitization is implied, but it is not their service. This mindset is little different from the DRE producers, who exacerbate the problem of inaccuracy and manipulation. Moreover, as disputes have arisen with the Voatz platform, their corporate identity becomes all the more apparent (Weinstein, 2019).

4.5.2 Security breach

Though the students appear to have approached viewed their actions with a 'friendly-hacker' mindset, that they did so during a live election landed them in deep trouble with the company and the U.S. Government (Weinstein, 2019). Voatz rebuffed any remorse for reporting two students to the FBI:

> "It is a standard practice for technology companies to report attack attempts to their clients and Voatz is contractually required to report such potential attacks during live elections – the same way an electric company would be required to report an attack on an electric grid to state and federal authorities, or a dam operator would be required to report an attack on software that monitors and operates dams to authorities such as the Army Corps of Engineers. Officials in West Virginia, in their discretion and independent of Voatz, then chose to refer the matter to the FBI (*Amicus Curiae* No 19-783, 2020; Warner, 2020).

This may be a fair legal point. However, if the Voatz platform is so weak that it cannot sustain investigations, sanctioned or unsanctioned, where does that leave us from a practical perspective? Another analyst observes, "…while Voatz portrays official bug-bounty testing programs as a superior alternative to unauthorized security research…Voatz's bug bounty program wasn't a viable option at the time Specter began its research" (Lee, 2020). Though we like to think that the legal realm reflects the practical one, they can be misaligned to the detriment of the average

citizen. If, indeed, the platform is hackable, that is the takeaway. Not whether it was legally hacked. It would be one thing if the project were still in its pilot phase. However, Voatz has been used in 70+ live elections. If it has not been compromised, it may simply be that no one has tried hard enough. (This dangerously resembles the 'security by obscurity' philosophy once used to defend the porous EVM software). The 2018 West Virginia primary attempted hackers were identified and associated with the University of Michigan from a specific computer science course (EECS 498) (Weinstein, 2019).

The students who attempted the hack are disciples of a cyber-academic named Appel, the man who hacked a Sequoia AVC Advantage DRE within 7 minutes (White et al., 2022; Weinstein, 2019). Appel is also close colleagues with Ed Felton. Felton, a giant in the computer engineering arena, is a controversial figure in the digital legal realm for various ethical hacking experiments of his own. Felton is also the director of the Center for Information Technology Policy at Princeton and serves within the White House Offices of Science and Technology Policy (White et al., 2022). Both Appel and Felton have come into legal trouble for rogue cyber investigations that some herald as genius, others felony.

The EECS course description that the students followed noted that 55% of the students' grades depended on "a large-scale group project related to a technical or tech policy topic on election cybersecurity" (Weinstein, 2019). Though the course description included the following disclaimer, it's most likely that the students' transgression was linked more to short-sighted ambition and curiosity than true malicious intent.

> "Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail

> time…Our class policy is that you must respect legal and ethical boundaries of vulnerability testing at all times, or else you will fail the course" (Weinstein, 2019).

Though this breach was unsuccessful (when it was detected, it triggered an automatic alert to the administrators as intended), what would have happened had a more endowed hacker attempted to compromise the system? Should Voatz be hanging them in the legal system, or should they have hired these kids? Reading between the lines, this department has a history of grooming eclectic yet top performers for government work in security. Pursuing this course of action may have created an enemy out of an asset. Moreover, would a malicious foreign (or domestic) entity ask before tampering with the system? Of course not. Abusers never ask permission. (*This applies to all genres of life). If history is any guide, when discrepancies arise in vote counting, this can create significant delays in outcome announcement, ignites demands for various recounts, and dismantle institutional trust even after order has been 'restored.'

4.5.3 Transparency

We notice here is that Voatz revives transparency questions of the same nature as the EVM manufacturers, who justified opaque behavior by citing DRE machine code as intellectual property. Though this is correct from a business standpoint because the systems were essential for national electoral infrastructure, this created severe vulnerabilities for over two decades. Voatz problematizes a similar debate, played out along different lines: independent security research (Lee, 2020). Voatz, as the most corporate dominant chain on the market, ignites the legal discussion about transparency, authorized versus 'unauthorized' auditing (hacking), sponsorship

influence, and the deep division between the tech world and capitol hill (Lee, 2020). Though part of the concerns presented by Voatz is that it emulates the corporate dynamics of its predecessor DREs, the remaining skepticism comes from a genuine concern about feasibility. In recent years, every experimental e-voting initiative launched in the U.S. has been muddled— not due to malicious intent but honest mistake. One might note the Iowa debacle of 2018 (Epstein et al., 2020).

'Debacle,' 'epic fiasco,' and 'disaster' are all words that have been tossed around to describe the Iowa 2020 caucuses (Epstein, 2020). It's become an infamous example of what one reporter describes as "why tech and voting don't mix" (Newton, 2020). Developed in partnership with a company called "Shadow Inc.," the issue of mobile app phone voting quickly devolved for two reasons (Kim, 2020). The first was a logistic failure, dubbed a back-end coding issue (Rosenberg et al., 2020). This dismissed longstanding red flags. Volunteers assigned to facilitate tabulation were put in a position where they could not have access to their smartphones for security purposes. However, the system was designed with a double-verification mechanism that required them to access a temporary code (sent to their smartphones) to begin their work (Kim, 2020). Though votes poured in, the volunteers couldn't begin (Epstein et al., 2020). The longer the verification process was delayed, the more incoming votes outpaced the personnel. While administrators convened to formulate a plan of action for the dual-verification and trouble-shooting the coding bugs, vote counting problems exacerbated. Shadow, Inc. was burned at the PR stake (Epstein, 2020; Kim, 2020). Though Shadow Inc. platform was a standard internet-based e-voting (not smart contracted to an anchor blockchain), its negative reputation ricocheted into alternative e-voting initiatives — such as blockchain-centric systems.

The second failure is that it quickly morphed into a partisan issue rather than

a technical one. Though Shadow, Inc. was highly problematic from a security perspective because it was relied upon for so long by various democratic activities that it cast its own shadow on the entire party— further polarizing existing dynamics (Epstein, 2020). The left looks over the fence at right-wing vigilantes storming the capitol, while the right looks back at the tech experiments gone awry (Kim, 2020). Meanwhile, both groups hurdle accusations about extreme lack of transparency, corruption, and systemic vulnerability to manipulation. These dynamics suffocate anyone wishing to remain moderate. Make no mistake: Shadow, Inc. should not be re-hired. However, that it became a party-polarized issue may stunt genuine progress in other theaters of technological development. Once again, transparency becomes a critical issue (O'Reilly, 2020; Rosenberg et al., 2020; Epstein, 2020).

Though the Iowa debacle is more recent in the collective memory of app-based voting initiatives, we might also recall the Washington experiment of 2016 gone wrong— the Democratic Congressional Campaign Committee (DCCC) hack (Moore, 2016; Weinstein, 2019; Bennett and Bender, 2016). Essentially, the entire experiment was shut down by researchers when it was hacked. After seizing control of the system, the hackers nominated and elected Hal 9000 (the authoritarian computer from the dystopian film "2001: A Space Odyssey" as mayor. Adding insult to injury, they also triggered the University of Michigan fight song to play whenever a vote was cast (the computer scientists who hacked the system hailed from U of M) (Moore, 2016). Their tampering didn't stop there:

> "…they changed all the votes to write-ins for famous robots and computers such as Johnny 5 (from the movie 'Short Circuit'), HAL 9000 (from '2001: A Space Odyssey'), and Deep Thought (from 'A Hitchhiker's Guide to the Galaxy')" (Moore, 2016).

Though they did so with a comic, Sci-Fi spoofing signature, the underlying implications were quite dark: ceding your sovereignty to a vulnerable cyber-system out of convenience— rather than merit—is to sell that sovereignty to whoever can outsmart it. One of the computer scientists (and assistant professor of computer science and engineering) who played a critical role in the hack notes:

> "(We) found that we could gain the same access privileges as the server application program itself, including read and write access to the encrypted ballots and database…Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters' secret ballots" (Halderman, 2016)

Through his blog, "Freedom to Tinker," he explores the gray area issues of information and technology policymaking (Halderman, 2016). Though his role in the attack was to highlight a critical security concern rather than maliciously attack the platform, the demonstration is quite powerful. Public examination is a *vital* component of transparency— the type of transparency we haven't seen from Voatz. Though disheartening for election officials, the breach, is precisely what made the experiment a success.

Despite significant problems in the prevalent tabulation system, it is far wiser to continue the development phase (rather than rush implementation) of Voatz. (This becomes more apparent when the case studies are analyzed in a comparative setting). Prioritizing paper, where possible, upgrading the DREs software, and updating the EAC certification standards are the steps that should be taken until either Voatz addresses its critiques or a better blockchain-based e-voting alternative emerges. However, these issues reinforce the conclusion that we should not implement this technology in an expansive live setting. Voatz argues that advancements addressing

key issues have removed the basis of these concerns. Skeptics reply, not enough.

4.6 Case study reviews and findings

The cases above are arranged according to the blockchain platforms (the chain) used rather than by the country, chronology, or some other metric. Doing so makes it more apparent that the chains themselves also mirror geopolitical fractures — such as Georgia's adoption of Exonum, the same used by the Russian municipal elections. Or KSI used by Estonia, sanctioned by NATO, and approved by the United States Department of Defense. These are not coincidental. Whether we consider them to be a manifestation of the path of least resistance or a more active form of alliance making (or cementing) is uncertain. However, technological adoption of this nature not only traces old lines but may create new ones. Might such developments bring Switzerland closer to Japan? Or push the United States away from Europe? Or pull satellite regions into Russia's technological orbit? Peering a layer deeper, we notice perhaps just how tight the tech community really is. Recall Juan Bennet, the co-founder of Chainlink, Protocol Labs, IPFS, and FileCoin. Who was his partner? Sergey Nazarov, son of Russian immigrants, became famous for co-founding ChainLink (with Bennet) and independently founding CryptaMail, and Secure Asset Exchange. If you were to take a moment to google this man's name, you would see numerous conspiracies that he is, in fact, Satoshi Nakamoto, the mysterious inventor of Bitcoin and the first blockchain. Though this has no verifiable basis, that it is even circulating in crypto lore speaks to the man's power more than his net worth.

Given this the depth of this tech relationship and Nazarov's possible connections to entities in the Russian tech scene, it also comes as little surprise why Protocol Labs served as an election observer for the Moscow City Council elections

in 2019. Does the link between Palo Alto and Moscow complicate, or at least texture, our understanding of emergent chains? What about the fact that the U.S. bureaucracy appears to be selling its soul to Voatz while Moscow is making use of its partnership with the California-based tech network instead? Perhaps it paradoxically dilutes the importance of nationality and heritage when developing systems for national security. This lesson is not taught by Nazarov or other tech gods with international roots but by Voatz, the homegrown incompetent.

Though technological dispersion plays a significant role in increasing interconnection, that does not mean that mirroring a smart-contract registry anchored to a public chain shared by another country's system requires you to share your registry information with them. Sensitive data, if localized, is out of reach. Moreover, mirrored infrastructural systems create venues for dialogue and mutual problem solving of respective issues. It essentially creates similar (though not identical) ecosystems of technological need. The more similar these infrastructural needs are, the more communication flourishes on the mere basis of a collective desire to troubleshoot. Especially for open-source projects, no one can use it if it doesn't work. Opportunities for international cooperation and interconnection exist today due to tech that has never existed on such a scale at any point in history.

Throughout this manuscript we identified how we arrived at our current tabulation system, assessed the vulnerabilities in that system, and analyzed alternative blockchain-based e-voting options in practice worldwide. Where applicable, we also discussed the key similarities and differences between the projects, scale potential, and general infrastructural elements of the various platforms. Here's the breakdown for the five cases in existence:

Table 6. Blockchain E-voting Experiments Worldwide

Host	***Chain/Anchor***	***Network***
Estonia	*Anchor:* Estonian Public Trust Anchor; *Service Provider:* Estonian Information Systems Authority (RIA); *Data Infrastructure:* X-Road	*Anchor:* Public, Permissionless *Data Infrastructure:* Permissioned
Russia	*Anchor:* BTC *Built/subcontracted by:* Waves Enterprise *Service Provider:* Rostelcom	*Anchor:* Public/ Permissionless *Data Infrastructure:* Permissioned
Switzerland	*Anchor:* Ethereum (ETH) *Data Infrastructure:* uPort	*Anchor:* Public/ Permissionless *Data Infrastructure:* Permissioned
Japan	*Anchor:* Uniswap (built on ETH+Binance SmartChain+HECO+Polkadot) *Intermediary:* UnilayerX (LayerX) *Data Infrastructure:* xID	*Dominant Anchor of the Anchor (ETH):* public, cross-chain transactions possible *Anchor (Uniswap):* public, but no cross-chain transactions *Data Infrastructure (xID):* Permissioned
USA	*Service Provider:* The Linux Foundation, Amazon, and Microsoft *Data Infrastructure:* Voatz (Amazon's AWS and Microsoft's Azure distributed across Hyper-ledger Fabric (HF) via 32 identical servers	*Anchor of the Anchor:* Hyperledger *Anchor (Hyperledger Fabric - HF):* Private and Permissioned, Enterprise/Modular

Source: [Author, 2022]

Looking at the case studies side-by-side, we can pull different lessons and insights from how each of these real-life experiments are unfolding. From Estonia, we see an interesting use of Web ID directories (X-Road) and strategic cooperation with supranational military alliances (NATO). In the Russian chain, we might note varying externalities from weak spots in the platform that were not remedied after

notification of these errors and accusations of data sales during the moments where the system briefly crashed. The Swiss portal conceptualization (uPort) relied on Smart Contracts to secure data locally prior to on-chain engagement creating perhaps the safest system for users. Similar structural features appeared in the Japanese Smart City system architecture. Like Switzerland, Japan focused on data management and election participation as one aspect, but not the central task which they sought to optimize. Lastly, in the United States, we see a reverse-engineered Android app reigniting the historic battle between corporate interest, national security, transparency, and privacy laws.

When reviewing existing literature on these blockchain-based remote e-voting systems and future projects, it's essential to note that there are several tiers of debate — and all of them are highly competitive. The first scholarly debate argues that voter-verifiable paper ballots (either in person or remote/mail-in) are the only acceptable means of voting. Those who are opposed advocate *not* for eliminating paper ballots but for including unverifiable (electronic) alternatives. This is the most superficial layer of the debate. One level deeper, the argument focuses exclusively on optimizing unverifiable (electronic) alternatives and whether in-person (DRE voting machines) or remote options (internet, mobile, and blockchain) are better. The third level of debate fractures the latter category. Their sole intention is not to do away with the other voter options but to optimize remote and unverifiable (electronic options) — the fourth quadrant (See Figure 3). These debaters argue over which of the three remote options — internet, mobile, or blockchain — presents the safest and most efficient mechanism for casting and verifying ballots. Amongst these three, blockchain has piqued the most interest and debate. Although both internet and mobile options have been heavily critiqued by all for insecurity, there is little debate

here. Nearly everyone agrees that any use of an internet connection invites vulnerability. However, among the three remote options, blockchain is the only one that has divided scholars and technical experts alike. One can find equal work applauding and condemning blockchain— but few peer-reviewed manuscripts between these poles. Suppose we lay out the puzzle pieces in front of us. We might see that the options available to us fit— more or less —into three conceptual categories. (See the table below).

Table 7. Categories of Tabulation Technology

Traditional	***E-voting Systems***	***Blockchain-based Alternative***
Paper-based	Electronic system	Electronic System
Physically or locally deployed	Fully Centralized System	Distributed System
The physical presence of voters and polling agents at the polling station	E-voting machines (EVMs), web connectivity if necessary	Web connectivity, as well as ICT infrastructure (Information and Communication Technology)
Operating costs every election, paper as physical ballots are required	Upfront operating costs are required first time, maintenance and troubleshooting thereafter	One-time ICT infrastructure operating costs
Huge political influence	Lack of political influence	No political influence (every node is represented by a hash)
Transparency lacking	More transparency	Greater transparency
Lengthy procedures, delays in result output	Output result is significantly faster	Real-time results

Source: [Hassan et al., 2022]

The division amongst experts regarding policy action— whether or not to pursue blockchain-based e-voting alternatives— cannot be understated. However, reviewing this ongoing scholarly debate, it appears that the greatest resistance to using blockchain-based e-voting systems emanates from the concerns over vulnerable internet connections (i.e., the same concern that applies to all voting means in the lower right quadrant — internet, mobile, and blockchain voting). Even supporters of

blockchain systems acknowledge that “Although decentralization helps solve many of these problems, the system cannot prevent all possible types of electoral fraud” (Gonzales et al., 2022). Bearing these cautions in mind, this project aims to identify a few viable means of moving forward (safely) with the technology. It’s also worth noting that exploring and testing these options does not equate to immediate implementation. It’s possible that, in the future, a parallel verification system could operate independently of the current tabulation protocol. Nonetheless, the issue of securitizing voting systems through alternative blockchain mechanisms remains a highly complex combination of geopolitical layers, technological advancements, paired legal constructions and crevices, and the additional mystique of uncharted territory.

CHAPTER 5

RISK ASSESSMENT

Most of the literature surrounding blockchain-based e-voting systems is either polarized, descriptive, or about a specific country case study. At the crux of the scholarly and policymaker debate is opportunity cost. Despite the flaws of the former hybrid system (paper ballots and EVM/DRE voting), emerging blockchain alternatives need to be vetted further before full-scale implementation. Among those who have helped contextualize the crisis of elections are Kosmin, 2015; King, 2016; Norris, 2020; Asenbaum, 2018; White et al., 2022; Abdollah, 2019; Epstein, 2015; Schneier, 2004; Bardhan, 2021; Rainie et al., 2021; Salehyan, 2014; and Specter et al., 2021. Others, such as Lien et al. (2016), outlined aspects of the split between the tech community and Washington D.C. alongside those who focused explicitly on e-participation, governance, and trust (Spirakis et al., 2010; Tambouris, 2015; Tsahkna, 2013; Zawicki et al., 2018; Asenbaum, 2018). Likewise, there is a growing selection of neutral literature that offers either technical resources (Ahmad et al., 2018; Khan et al., 2021; Prakash et al., 2016; Wegryzn, 2021) or an assessment of blockchain's status in governance infrastructure and its open-ended issues (Casino et al., 2019; Gan et al., 2021; Pelt et al., 2020; Serdült et al., 2015; Aouidef et al., 2021). While all the above resources and others contribute to our overall understanding of the nature of the voting system dilemma, scholarly literature on the topic splits when it shifts from descriptive to normative. (The former adds texture, and the latter offers a policy direction).

On one end of this spectrum are the enthusiasts; they view the prospect of blockchain-based e-voting systems with overall optimism (Anwar ul Hassan et al.,

2022, Gonzales et al., 2022; Kassem et al., 2019; Alessie et al., 2019; Jafar et al., 2021; Khan et al.., 2021; Meyer, 2018; Shovkhalov et al., 2021). The other perspective end is marked by reluctance, skepticism, and concern of varying intensity (Schneier, 2015; Norden et al., 2018; Park et al., 2021; Epstein, 2021; Casey et al., 2016; Rosenburg, 2020; Theilman, 2015; Weinstein, 2019; White et al., 2019).

Those manuscripts that present in 'neutral' language tend to be more tech-centric, focused on either solving for or explaining how the pieces of the puzzle fit together, which offers little normative direction for policymakers. Insightful as they are, the resources with the most organic empiric information tell us what we *could* do, not what we should do. Many normative pieces instructing what we *should* do often lack the technical background to do justice to their own recommendations.

Interestingly, tech experts and cybersecurity specialists appear to share the same goal yet harbor opposing stances. Developers are attracted by the challenge of optimization as much as cyber specialists are vigilantly trying to limit the introduction of new vulnerabilities that may be far worse than those we currently face. Regardless of their normative conclusions, all of these works contribute to understanding the current policy dilemmas many governing institutions face when confronted with technological developments. Unfortunately, that 'understanding' is split down the middle.

> "For more than a decade, it has been an elusive dream for election officials: a smartphone app that would let swaths of voters cast their ballots from their living rooms. It has also been a nightmare for cyber-experts, who argue that no technology is secure enough to trust with the very basis of American democracy." (Rosenburg, 2020).

As we begin articulating a coherent risk assessment, it's essential to consider the

opportunity costs of moving forward. These nascent developments have the potential to empower citizens or enslave them. So, when we discuss 'moving forward,' even this can be met with resistance depending on its interpretation. On the other hand, if 'moving ahead' means focusing on strengthening a pilot project and beta-testing, this does not pose an immediate threat. Due diligence and testing should be done to ensure that — in the future— if such systems are put into practice, they have been vetted slowly and methodically. If 'moving ahead' means scrambling to put a product on the market before anyone else and reap the rewards, regardless of whether it is ready, then the hair should prickle on our necks.

> "What good is it to vote conveniently on your phone if you obtain little or no assurance that your vote will be counted correctly, or at all?" (Park et al., 2021).

Given that blockchain-based systems have already taken root in various ecosystems, it is wise not to be negligent when it comes to developing policies that will set for precedent future election cycles and new data management systems in governance (Pelt et al., 2020; O'Reilly, 2022; Aouidef et al., 2021, Katsh and Robinovish-Einy, 2021). Whether one finds themself in favor of maintaining the status quo or the opposite (upending it by embracing alternatives)— the middle path would acknowledge that both venues carry different opportunity costs. Localized tabulation introduces localized problems (a higher probability of manipulation but smaller scale potential for damage from any given breach). Centralized tabulation, one might expect, should have a lower likelihood of manipulation but the potential for the entire outcome to be modified from any given breach. These are the two extreme ends of the scale. Some (not all) of this risk is mitigated by a hybrid system (offering the

opportunity for both traditional (paper) and e-voting (DRE) options.

This dynamic is one of the problems we see the uPort (Switzerland) and LayerX (Japan) solve by using smart contracts to localize users' personal data and encrypt it in separate external (off-chain) sites (encrypted in the dApp on the user's device and the in the offline municipal registry).

5.1 Risk absorption

Although any adaption of blockchain tech to electoral and data systems would inevitably adopt the DLT (distributed ledger) rather than DEX (distributed exchange) infrastructure, some common crypto critiques do carry over. For example, Park et al. (2021) noted: "Cryptocurrencies have fewer risk-absorption mechanisms than traditional banking; losses often fall directly on the victims, with no third party to provide relief." In a DLT-oriented system, rather than a crypto exchange platform, the concern that users will bear an asymmetric burden if the system is significantly flawed should not be dismissed as the paranoia of a few skeptics. Implementing blockchain-based e-voting systems will impose different burdens depending on development tiers, regions, countries, states, and even ages. What we're left addressing then is a net benefit. What is it, how can externalities be mitigated, and are the gains worth the sacrifices?

If we were to invite every scholar referenced to a party, would the room erupt in discord, would hard lines soften, or soft lines harden? It's impossible to know. For example, Hassan et al. published a piece that began with a similar logic to this manuscript. On voter fraud and ballot manipulation, he asserts, "blockchain technologies solve this problem by providing a distributed ledger with immutable, encrypted, and secure transactions" (Hassan et al., 2022). Though many might

disagree, he simply aligned his team's paper with a category of 'affirmative' literature— a manuscript supporting continued development in blockchain-based e-voting systems. Though controversial, this is not what Hassan intends to problematize; instead, this is a starting assumption. The broader premise of his research team's paper argues that such blockchain solutions should be implemented in Pakistan. Suddenly the entire nature of debate shifts. What began as a general question (can blockchain reduce electoral corruption?) suddenly became more specific. Is it premature to introduce such initiatives in a developing region with gapping security vulnerabilities, or is this the medicine? Does it invite risk or recovery? Would it worsen asymmetry or mitigate aspects of it? These analyses indirectly initiate the scholarly conversation (or rather, debate) on risk absorption. On this macro-analytic level, we can tease out a bigger question. How would blockchain voting alternatives affect the multi-level asymmetry prevalent in developing and lesser developed regions?

5.1.1 Global asymmetry

On one level, there are global asymmetries between these regions and developed countries forever acting against developing and lesser-developed nations. The search for a solution to mitigate vulnerability to corruption and increase institutional strength is ardent because it increases competitiveness internationally. Domestically, more secure elections could correlate to greater social stability. Although the motivation between developed, developing, and lesser-developed nations are the same (e.g., reducing infrastructural vulnerability in voting systems), the conditions are studded with challenges of different intensities.

Implementing these solutions in certain developing regions presents extreme logistical and humanitarian concerns at a much steeper opportunity cost than if the

same solution were implemented in a country with a stronger rule of law. This does *not* imply that all developing countries are unequivocally 'sound enough' to implement these solutions either— Voatz proved that. It means that when something goes seriously wrong, it takes longer to run over people in a developed country because the legal system slows it down. The citizens of autocracy have no such barrier between the whims of their government and the consequences of infrastructural design failures. This puts citizens of developing and lesser developed regions at a more immediate humanitarian risk. If a flawed system is implemented in a developed region, it will still erode the institutions. However, the citizens of non-autocratic nations may not feel such consequences for generations, years, or months depending on the severity of design issues.

Moreover, there are heaping logistic dilemmas as well. Off-the-grid individuals with little to no access to digital devices would have no means of voting. Privileged individuals with access, education, and experience with computers and smartphones would enjoy apparent advantages. Even if the devices were provided to remote areas, how many would feel comfortable using a computer—perhaps for the first time in their lives? It would create even more significant domestic asymmetries in countries with a wide privilege gap. Such a scenario of imposing technology in an environment where that doesn't suit local needs would do far more harm than good.

Thus, if blockchain-based voting became the default in developing and lesser-developed countries, it would likely worsen political representation based on class more extremely than this might manifest in a developed county. This is not because the citizens in developed countries all enjoy equality—they do not. The concept of "equality" looks and feels different in the United States than in Switzerland or any set of countries in comparison. Likewise, though poverty manifests differently in

every context, the wealth gap is usually closer in developed countries. Developed countries do not have to logistically accommodate entire cities existing off-the-grid— it would be an individual basis.

Global and domestic wealth is a significant discriminating factor when creating solutions for election participation around smartphone apps. This could worsen existing economic asymmetries because not everyone has access to these devices. Age is also a significant discriminating factor. Older individuals are notoriously either unable or unwilling to adopt new modes of technology, yet they have every right to participate in elections. If voting took place on a mobile app— regardless of whether it's blockchain-oriented— it might be alienating for older demographics if ample traditional alternatives are not provided.

In some cases, such as Estonia, we saw that it did increase women's participation because of the time reduction. It's plausible we could see trends like this emerging elsewhere, but it's still too soon to measure the remaining cases for eParticipation on gendered lines. Moreover, it's not enough to simply think of macro-analytic development tiers, regions, countries, and states. We must also consider the meso and micro-levels, such as wealth, gender, and age. Thus, transitioning to blockchain-based e-voting systems may impose differing externalities on individuals — even within the same household. Whether the net gains outweigh the costs (or if a ready solution can be implemented to reduce barriers to access for certain groups), these should be considered when forming pre-emptive and protective policy decisions on emerging blockchain-based e-voting systems.

5.1.2 Asymmetric sensitivity and vulnerability

Alongside fraud-proofing the system from external attacks, it is also imperative to

protect the users from administrators (Alvarez et al., 2009). As mentioned in Chapter 4, public blockchains are fully decentralized (and therefore immutable by government entities). Private blockchains are wholly controlled by whoever owns them to the extent that they can write or erase history on the "perfect record"– meaning that if a government owns it, then they own the users. Thus, some version of the permissioned network creates the best possible compromise between them. Likewise, anonymous node and network verification protocols operate to the advantage of user data protection. However, this convenience and comfort are likely to push aspects of our digital identity into, ironically, a more centralized format. For example, some countries (such as Switzerland via uPort) have applied permissioned blockchains to digital identity for everything from bike rentals and parking to municipal elections. Based on these trends, introducing blockchain for e-voting systems may introduce (rather than resolve) the hyper-consolidation of personal information if the constraints of administrative permission are too tight *or* the data is not localized off-chain (i.e., if no proxy ID is issued). One might also note X-road, a digital ID platform used to centralize personal data pioneered by Estonia. Since its original implementation, it is now being used in Finland, Azerbaijan, Namibia, and the Farro Islands) to centralize personal data (PWC, 2022). Likewise, blockchain is already playing a role in administrative governance beyond the electoral purposes analyzed in this manuscript. For instance, Alessie et al. identify "three broad service groups: public aid and social transfers; citizen's records and public registries; foundational components (identity and regulatory compliance)" (Alessie et al., 2022). These activities place Digital ID and Biometric verification at the center of technical, philosophical, and political questions.

> "…the political expediency of adopting a 'high-tech' solution also poses the risk that proposals may be too quickly pursued, before allocating sufficient time and funding for independent audits and feedback from security experts. New technologies should be approached with particular caution when a mistake could undermine the democratic process" (Park et al., 2021).

If the infrastructure developers do not respect the anonymity of voter data in the system design, this could create disproportionate risks for under-protected religious, ethnic, and gender minorities. The risk calculation for developing versus developed countries is different in the short, mid, and long-term. According to Nye and Keohane (1989), the two most important dimensions framing this risk assessment are "sensitivity and (2) vulnerability."

> "Sensitivity is the speed and magnitude with which a change in one country is felt in another within one policy framework." The policy framework is constant. Vulnerability is the relative availability and costliness of alternative policy frameworks when it becomes necessary to adapt to external changes… Vulnerability interdependence is more important in providing power resources to actors; with effective alternatives, sensitivity effects can be overcome… vulnerability can take on a strategic dimension, as less vulnerable states can impose costs on others by exploiting their sensitivity. Sensitivity can also pose problems for leaders of [pluralistic] political systems when interdependence harms domestic groups that will subsequently clamor for protection from the government" (Keohane and Nye, 1989).

In this case, technical blockchain knowledge of the systems that curate elections could be viewed as a significant source of soft power. Sovereignty over tech capabilities, rather than dependence on knowledge sharing or support from another country's system, may have significant consequences for countries with capital or skilled labor deficits.

Moreover, the path of blockchain-based e-voting has not yet proven to be

safe, even in countries that market themselves as stable. The United States itself—which devoted years of pathos and invasion to democracy-building initiatives—- is setting infrastructural foundations for a premature system with arguably the least user protection. My hesitancy to agree with Hassan (who advocated blockchain e-voting for Pakistan) is because fragile infrastructure amplifies the inherent vulnerabilities of introducing new infrastructural components (such as blockchain e-voting). Given the extreme global tech disparities, it would also pit Pakistan into a position of greater dependence on an external entity to develop a system that many citizens might not be able to access. Domestic technology disparities would become more acute as well. For example, the Federally Administered Tribal Areas (FATA) would be even more disadvantaged from their metropolitan counterparts than before. Hassan is not alone in his idealism, and — if optimism drives investigation— this may not be a bad thing provided that pragmatism finds a home in the analytical conclusion. Worldwide we find ourselves confronted with prevalent systemic flaws. It's quite easy to say the equivalent of, 'anything would be better than this.' However, are we absolutely certain that this is true in the case of blockchain voting? It's too early to tell. Colatin (2022), who pioneered research in international law following the Estonian cyber-attack, or Ansper et al. (2010), who analyzed e-voting as a security concept, might agree that time and more thorough investigation are needed.

If the conditions of stable liberal democracy are met, using a parallel blockchain-powered electoral verification system may offer a venue for improving the critical metrics: accuracy, anonymity, scalability, and speed. But even this is no guarantee. So, can blockchain reduce electoral corruption? Holding all variables constant, yes, blockchain *can* reduce electoral corruption. But what of the unforeseen variables impossible to control for? That this is uncharted territory is more reason to

continue development and delay live implementation. More time is needed to address these variables and securitize them. If development is rushed for the sake of implementation, the consequences will be severe— regardless of the base level of privilege enjoyed by the implementing country.

5.2 Transitioning from numeric to biometric identities

For better or worse, our identities are becoming increasingly digital. Anyone who possesses a national ID, a passport, a driver's license, health insurance card, a student card, Social Security Number (SSN), a birth certificate, a death certificate, or any other form of identification already possesses a numeric identity. That is, a verifiable number associated with one's being in society. Granted, not all are transferable over national borders; some have expiration dates, and they possess different forms of prestige, but all essentially condense your human identity into something numeric. (Note: death certificates *are* relevant to his dialogue because, if you remember, the dead frequently "vote"— more so in controversial elections).

In the United States, the transformation of our identities to a numeric entity became most firmly entrenched with Social Security Number (SSN), which effectively converted characters (the letters that form our given names) to numbers (that can be codified and categorized more easily). This is required for all major activities and was once considered more sacred than a passport ID. In Turkey, the e-devlet is comparable to Americans' SSN. Any Turkish resident (foreigners and citizens alike) must be accompanied by a kimlik, or national ID card, to prove their legal status in the country. No sovereign, internationally recognized nation omits the practice of numerically verifying its own citizens to the best of its efforts. For better or worse, numeric verification is a halfway point for the full digitalization of our

identities.

What is digital identity? Digital identity comprises any collection of information traceable to you. Informally, this can include personal data of any level: "photos you've uploaded to social media, posts you've created or commented on, your online bank account, search engine history…" (Avast, 2021). Countless invisible entities make money from buying (and capitalizing on) massive amounts of personal data— collecting through legal and illegal means. The reason being that comparably few legal protections exist in favor of the individuals being bought and sold.

Our comfort with a world curated by algorithms (everything from our Spotify to Twitter profiles, for example) is mainly due to mass computations made on unguarded personal information. Algorithms work to our benefit so often that their abusive shadow side receives less attention. That data acquisition is such a silent theft makes it more pervasive. We might full' digital identity, in a general sense, to be 3/4 point to full digitalization. By "full," I mean centralizing numeric, digital, and biometric aspects of our identity. If that doesn't raise a few hairs on the back of your neck, perhaps it should.

More and more individuals are being encoded into systems on biometric terms. From frequent flyer registrations to criminal records, fingerprints to eye scans, biometric identifiers are replacing serial IDs. If one wants to live integrated within any society, they have no choice but to possess a verifiable identity (numeric, digital, or otherwise) to lead a "normal" life. (Arguably, "normal" no longer exists). The shocking absence of personal autonomy today's global citizens face is a double-edged sword, where one side of the blade is collective security and the other vulnerability and dependence.

The need to open a new bank account when moving from one country to another will be obsolete for the same reason that voting in national elections overseas need not pose an issue. Digital identities are trackable anywhere. While it may bring greater convenience, it comes with an irreversible price. Moreover, in an environment monitored and curated by tech giants and unmitigated data mining, the only persons who might possess true digital freedom, ironically, are stateless individuals. However, the costs of being stateless are so steep most would assert that it is anything but "free." Even "inalienable" human rights are curated and protected by the state to which individuals belong. If no state assumes responsibility for a citizen, they are at risk of falling through the cracks of society–regionally, nationally, and internationally. However, some experiments with blockchain-based identification systems refugee camps have been among the first not only push the boundaries of unidentified statelessness while also stirring dystopian concerns.

Regardless of the humanistic rhetoric or ethos that inspired these systems, increasing experiments often involve vulnerable demographics (refugees) or groups who have no right to reject participation (military personnel); the lack of genuine consent in the pilot testing is alarming. The concept of technological determinism packs a punch only if consent is stripped— and, indirectly, this is not uncommon (Dusek, 2006; Doboli and Umbarkar, 2014), and Vermaas et al., 2011). Though the dystopian narrative sells Sci-Fi books and movies, scholars are less likely to discuss "tech takeover;" rather, they analyze situations of consent relinquished, surrendered control over the development process, lack of transparency, and apathy over the evolution. The voluntary (or imposed) adoption of a passive role in the evolution of social infrastructure might shift the relationship between society and technological infrastructure from a social constructivist dynamic to a deterministic one. Feenberg

(2017), for example, describes it like this:

> "To say that technology is autonomous is not of course to say that it acts alone. Human beings are involved, but the question is, do they actually have the freedom to decide how technology will be applied and develop? Is the next step in the evolution of the technical system up to human decision-makers or do they act according to a logic inscribed in the very nature of technology? In the latter case technology can rightly be said to be autonomous. On the other hand, technology would be humanly controllable if we could determine the next step in its evolution in accordance with intentions elaborated without reference to the imperatives of technology" (Feenberg 2017, p. 10).

This passage is not intended to demoralize but rather to inspire active work in privacy laws and the right to anonymity, particularly in data-centric elements of national infrastructure such as voting systems. Since the dawn of the tech revolution in the 1990s, the world has seen a numbingly repetitive pattern. In which, technological development outpaces legal protections designed to safeguard users' civil rights. If any takeaway should be drawn from this project, it is not that it is possible —it is — but that little to no pre-emptive action has been taken to protect the civil liberties of individuals with biometric registration on these future chains.

Consider the trajectory of biometric verification. In the US, one of its earliest uses was to identify criminals. In other words, the lowest ranks of society lost the freedom of privacy or anonymity within their lives. (Does this not sound at least somewhat familiar to the San Bernardino case where user protections were hacked because the user was a known terrorist)? The familiar rhetoric "freedom of privacy" is misleading as it implies it is somehow inalienable. From a legal standpoint, it has been treated as a de facto privilege but not a birthright.

Moreover, it is a privilege that fewer and fewer people enjoy— regardless of

their criminal status. It is a sobering paradox to consider that, due to technological advances, the average law-abiding 21st-century individual lives with fewer privacy freedoms than yesteryear's criminals. Today, fingerprinting has lost its sole association with criminality. A basic TSA pre-check requires all ten fingerprints registered with one's passport. Yet, from retina scans to machines reading the veins of the palm, our biometric identities are increasingly relied upon as a baseline identifier, as is the rising use of facial recognition cameras (as anyone at Boğaziçi can attest).

Another example is genetic testing. The relative inexpensiveness of a complete genetic workup compared to the equipment expenses, degree of specialization, and the value of insight provided about one's complete genetic makeup is also a red flag. Individuals issuing such tests are likely not the sole recipients of the results, and it's quite possible that the bulk of this data is sold to medical research companies. If it contributes to positive developments in the field, many might be asking, what's the problem? The problem is you don't know if they are the only customers.

The underdevelopment of biometric data privacy laws may make it easy for award-winning researchers to access your data, but what if it's sold to your insurance company without your permission? Suppose you have a recessive predisposition to heart disease. Might you be less likely to receive health insurance despite your healthy exercise habits and good diet simply because companies don't want to take a risk on you? In this example, the nature-versus-nurture discussion is dislocated into a business model. Is it out of the realm of possibility to consider whether governing and intelligence authorities have considered linking biometric, civilian, health, and — if accessible— voting information in a centralized space? Every action begins as a thought.

5.3 Opportunity costs

What are the trade-offs? Placing national security front and center obliterates civil rights of privacy. Have we not been down this road before? In 2013, U.S. security agencies collected twice as much data on their own citizens compared to, for example, Russia. Yet, a decade into this revelation, we still live in a world in which very little is illegal when it comes to data protection.

If history is any guide, the rate of technological advancement does not spell a long wait before blockchain-based electoral mechanisms are used on a more routine basis. This is not an ominous forecast; it is merely the forecast. If one were to adopt the game-theoretic view proposed by Axelrod and Keohane (1985), policymakers would be wise to structure situations of convergence (such as bug bounty programs or hackathons) where repeated cooperation could pave the way for future collaboration. Armed with this knowledge, it may be possible to dodge the negative externalities with proper legal preparations regarding data protection and legal arbitration for disputes. Such entities may exist. If so, this is where the academic gaze should be directed in future works— the legal dimension. It's imperative to recognize we are all standing on the cliff of major technological changes. These changes could prove to be instrumental in increasing confidence in election results.

Mishandled, they could irreversibly strip citizens of personal freedoms. Preparation determines the outcome. Inappropriately applied, a blockchain-based electoral verification system running on the basis of biometric citizen identifiers could be catastrophic if it were applied to a closed chain system wherein the curating entities (a government administration, for example) have full autonomy over it. Complete control over the leger (in a fully private chain) means that— in theory— data inputs could be retrospectively changed by those who manage it. This would create an

entirely different, technocratic brand of authoritarianism.

With that said, there is also the possibility that because most systems thus far rely on a public anchor chain — open-source, able to be contributed to and audited worldwide) with only localized data stores, it's possible that such a scenario could increase interdependence. This would mitigate the risk of the political 'doomsday' scenario mentioned above.

"As an analytical concept, interdependence refers to situations where states or actors are determined by external events or entities (e.g., an external blockchain anchor) in a reciprocal relationship with other states or actors, jointly limiting their autonomy. It is created by expanding international transactions insofar as the costs associated with them constrain political activity. While these relationships impose costs, the benefits may exceed them" (Nye and Keohane, 1989).

5.4 Autocracy, fintocracy, and technocracy

Suppose we step back from this extreme scenario and look at this from a historical perspective— not like we did when retracing the evolution of EVM technology — but from a wider conceptual lens. At the crux of each scenario, we have looked at the implications of centralization versus decentralization. From hacking dilemmas at polling stations (targeting central databases) to selecting which category of blockchain might be appropriate for electoral purposes (a permissioned registry anchored to a public chain), a core consideration is mitigating the propensity for hyper-consolidation of power. The data doomsday scenario becomes a risk if elections are conducted through a private chain, not anchored to a public, open, decentralized entity. The principle of the blockchain-based e-voting system implemented appropriately would actually redistribute verification from a vertical

model (client-server) to a horizontal one (P2P). Thus, the first paradox we encounter is this: if decentralized ledger technology (DLT) is abused, blockchain-based systems can become a technocratic tool for those wishing to centralize power further.

The most evident risks exist when extrapolating cybersecurity policy projections according to regime type. How would this technological capability unfold in flawed versus full democracies? One might expect the degree of democracy to determine the level of citizen cyber protections (rather than the other way around) within a certain range. Technology often acts as the independent variable— an influencing variable that can elevate a situation from bad to better— when other institutions are reasonably sound. Technology becomes a tool of oppressors — a scenario where its development is not embedded with citizen protections and where is development is heavy-handed — when other institutions are not democratically aligned. Thus, the capability of certain technologies (blockchain e-voting included) to improve security may be more dependent on the strength of existing political institutions than a moving force itself acting to bring those institutions into line.

On the more extreme end of the spectrum, in hyper-authoritarian countries, cyber-securities may not be granted by a political system with any history of protecting citizens physical security, let alone their digital security. When regimes are not necessarily open to scrutiny and participation, how they can actually be endangering citizens if some who their data is made public or is available to the ruler at the end? Likewise, a sense of helplessness might manifest in a lack of political will to protect that data — or to try. If such societies are confronted with this technology, how will that data be used if they cannot or do not have the political will to demand personal data protections? It's uncertain. More complicated still, what happens when citizens of an authoritarian country are hired by their own governments to craft a

system they know will restrict their own freedoms? Perhaps the answer lies again in engaging international third parties and entrusting them with the controller IDs (see chapter 4) instead. This would mean that the most sensitive data (anything that could harm the citizens' it belonged to) would be parceled and secured in distributed pockets overseas — essentially hidden from the regime itself. This would necessitate coordinating with international organizations and pre-emptive policy work priming countries to seek cooperation rather than view it as an imposition.

The second irony we see is historical subversion. On some level, it's plausible to consider that decentralized exchanges (DEXs) emerged as a competitive response to dynamics put in motion by the financialization movement of the late 70s and 80s. The phenomena of financialization in the 1980s gave rise to previously unheard-of structures curating financial capitalism. Unlike industrial capitalism before it, which relied upon commodities, financial capitalism built structures that recycled wealth itself. The propensity for profit in a financialized system was not tethered to a material product. When one thinks of the giants of industrialized capitalism, Standard Oil or General Motors comes to mind. They rely on material resources and exporting a product for consumption.

Further, financial capitalism fans its palm leaves to Wall Street bankers, investors in Hong Kong, and others in pursuit of profit via the buying and selling of financial products. Currency, stocks, bonds, and other derivatives are intangible. They cannot be eaten for nutrition, burned in the winter for warmth, or 'used' in any practical way other than as a means for wealth accumulation.

Though this is a technical (not financial) project, the evolution of fin-tech (as a product of financialization) is useful for understanding the basis of blockchain and why it lends itself so easily to transacting value—data of any kind (monetary or

otherwise). Financialization demanded new technological infrastructure. These introduced an uncharted outlet for systemic reform that is unlikely to be ignored as former systems become less and less able to accommodate contemporary market needs: quicker and easier international transactions, greater security, and the form of less trust and more verification. Kotz (2008) explores the 1980s as a critical timeframe of transition in which state-regulated capitalism shifts toward neoliberalism. Around this time, Kotz also notes the rise of 'complex types of securities; ' created and traded, bought and sold that emerged alongside the asymmetry between profits derived from non-financial activity (such as the production, storage, distribution of goods, and service production classified on a non-financial basis) as opposed to the products of regular financial activity (dealings in stocks and bonds, mortgages, financial derivatives, futures, foreign exchange) (Kotz, 2008). In this schema, financial derivatives (value tied to the value of other securities) also fall into the latter category. Throughout this time, massive social structures of accumulation (SSA; asset wealth) swelled predominantly in the countries expounding these neoliberal policy prescriptions, exacerbating global asymmetries as well as domestic asymmetries in countries where neoliberalism trended (Kotz, 2008). The growing lust for profits of financially driven activity over steady but laborious non-financial activity is the backbone of financialization. The birth of financialization is often attributed to a combination of these policies and new technological infrastructure invented purely for financial asset building. This new infrastructure came to be known as "Fin-Tech." As the hourly or salaried worker became less and less able to compete with passive accruing assets, the wealth gap widened.

Thus, financialization is interwoven into the very genetics of corporate

capitalism, which is a very different story than the rags-to-riches philosophical interpretation of capitalism promoted by "The American Dream." If that still exists, it's owed to the strong rule of law, but this as a standalone philosophy is structurally obsolete in today's United States of America. Financial activity is consolidated on the coasts, and non-financial activity occurs in the middle — derogatively known as the "fly-over zone" by the North American elite. It is this breed of corporate capitalism that dominates U.S. politico-economic culture. Likewise, because capital always seeks to escape risk, it seizes the opportunity to obtain both power and protection: monopoly, if available. One facet of the crypto origin narrative uses its rejection of monopoly and hyper-centralization as a fundamental starting point. Economics is strictly concerned with production, consumption, and how to manage these activities through supply and demand. Finance juggles funds, investments, and cash, all while timing entries and exits from the market according to risk. Finance is less concerned with productivity and more focused on money flow. That means the infrastructure that rises around these endeavors (i.e., stock exchanges) is far different from the economic structures (i.e., fiscal and monetary policy, central bank decisions, etc.). Because both are hyper-concerned with "the market," economics and finance are often confused interchangeably. That they work in tandem illustrates they are *separate* entities. These separate entities have nuanced needs. As the saying goes, necessity is the mother of all inventions. Blockchain was an invention of (nontraditional) financial necessity. The attractiveness of nontraditional digital assets is alluring to individuals and entities who have lost their appetite for high interest rates, inflation, and the growing disconnect between hourly and salaried wages relative to living costs. At the root of their complaints are socio-economic and politico-economic gripes that have been intensifying for decades. Thus, economic

theories cannot be ignored — nor can we consider them separate from political ones.

The popularity of neoliberal policy created ideal conditions for the phenomenological rise of financialization (Kotz, 2008). This pairing reinforced asymmetry over equality, thus creating an environment financially alienating anyone *not* involved in traditional finance (or a highly lucrative industry). Thus, disenchantment (at least in part) yielded the birth of an alternative financial structure out of reach from the traditional sector: digital asset finance. Decentralized, it lives outside the realm of traditional finance but mirrors aspects of the finance realm and that of politics. To play the devil's advocate, it's possible the crypto and blockchain realm has created a new level of wealth alienating traditional finance —or created a new venue for individuals already versed in the financial world to jump ship to something more lucrative. Crypto has the capacity to dislocate and empower simultaneously. Nonetheless, our focus is blockchain— the architecture.

The democratic consensus mechanisms embedded in the chain upgrade protocols of the chains that support these transactions are one example of political reflection. Consensus protocols mirror the ethos of a cooperation-driven liberal institutional approach in a way that can (if wielded appropriately) offer results in a way that political rhetoric has come up short. These same slogans that offered cooperation, democracy, and cosmopolitanism have delivered increased polarization, sliding democracy rankings, and isolationism. This disconnect drives exploration, and it can be healthy—if desperation does not rush it. The lack of existing international rules, laws, and regulations on these is as intriguing as it is concerning (Katsh and Robinovish-Einy, 2021). Built-in consensus and an immutable ledger might be the only traditional aspects of blockchain-based tech that fit into traditional conceptions of political theorists. Yet, despite increasing affirmations of legitimacy

from government entities, there is still respectively little regulatory depth (O'Reilly, 2022).

Further, the very prospect of using blockchain and smart contract registries illustrates that, on some level, we can repurpose financial structures (or their features) into political infrastructures; it also shows that some political features (i.e., democratic consensus mechanisms, smart-contract preconditions, node equality, etc.) are directly embedded in the functionality of these blockchain-anchored platforms. Among the many paradoxes within this project is the suggestion of recycling a strategy of the rebel child (decentralized verification, De-Fi, and DLTs) whose parents (traditional finance, financialization, and wealth inequality) bear some blame for eroding trust in political governance institutions (such as electoral systems). Experimenting with blockchain alternatives confronting election insecurity is like splicing a gene from the DNA strand of one problem (fintocracy) and using it to engineer a solution against a different threat altogether (autocracy). However, the ability to accrue passive assets is not problematic; when a limited group wields vast knowledge and resources relative to the average population, this creates "Fintocracy"— wealth-centric power. Autocracy typically implies a monopoly of violence — oppression-centric power.

Yet, there is a third category which is not yet gained eminence, and that is Technocracy. There are some fears that an oligarchy of tech-savvy individuals or countries with a higher distribution of tech-savvy citizens may wield such an advantage that this would lead to the newest face of absolutism in the modern world: technocracy. Though there's merit to the implications of this concern (greater domestic and global asymmetry), there is a noticeably greater dispersion of knowledge worldwide in the crypto and blockchain community than in the era that conceived

traditional fin-tech. This is because the decentralized nature of blockchain development is open source. Thus, the code is accessible to everyone with access to a computer or smartphone. (The inequalities that stem from lack of access to technology is a larger issue; these individuals are already disadvantaged in more ways than this manuscript has time to address). The takeaway here is that financial structures can be adapted and recycled back into politics as much as politics can be recycled into adaptations of the previous financial structures.

5.5 Supranational brokerage

The next question worth asking is: is this system safe to implement on a strict domestic basis, or should it be brokered by an international institution? In the future, supranational brokerage options might provide citizens with a means of protecting themselves from their own governments. Supranational involvement could also help compensate (through membership and alliance) for otherwise fatal power asymmetries, such as Estonia seeking assistance to thwart cyber-attacks from Russian origins. In this example, NATO membership became vital. However, what other international organizations might prove to be influential players? (UN agencies, ICANN, etc.).

At some point, it does not matter whether we prefer or decide that paper ballots are better. At some point in the tabulation process, the ballot that leaves a voter's hand is digitized and centralized. They may not see it, but this is what happens. Assuming otherwise is to take comfort in a false sense of security. Thus, even if paper ballots are promoted, we still face the same critical issues of web connection and a vulnerable (hackable) centralized database after those ballots are digitized out of sight. When your place all your eggs in one basket, dropping that

basket means you lose all your eggs. If the aim is to avoid a one-breach wipe-out (or mass manipulation of votes), perhaps we should not take as much comfort as we've been taking with paper ballots.

The capacity to issue server-side credentials (decentralized, government-issued ID) means that registering and tabulating votes casts is entirely possible. Few can argue that blockchain presents a compelling option, but what opportunity costs have we identified so far? Another question worth asking is, can we truly 'decentralize' security, and if not, what are the caveats? The first question looks outward (toward potential external threats), while the second looks inward (at the risks citizens face from their own governments). To build an appropriate system, it's imperative to recognize that there is a perennial risk from both sides. Where these two opposing pressures meet is the boundary point.

As we sift through the pros and cons of whether or not blockchain *should* be used in one context or another, it's worth noting that the cost of failure, depending on the country, does not fall equally on citizens and the nations that attempt them. In nations with a lower institutional strength, the cost of failure will invariably be higher for citizens of that country. The incidence of internal corruption of the system is higher (which would result in greater oppression of the citizens) and might further entrench whoever is heading the administration. In institutionally strong(er) countries, the nation will likely pay a higher cost than the individual. This does not imply that these citizens are untouchable — only that when they feel it, it may be too late.

Moreover, if volatility persists in institutionally strong countries acting as regional or global hegemonies grounding political stability — it will ripple widely. In other words, failure — for developed, developing, or lesser developed nations— has

the potential to be catastrophic. The cost of rushing comes with a higher risk of failing.

With that said, many countries, the United States included, are already failing in a different system— a hybrid of the traditional paper ballot (localized counting) and e-voting techniques using outmoded EVMs (centralizing databases). It's essential to recognize that choosing the status quo is a decision in itself. If this is the path taken, policymakers should at least consciously select it rather than do so by accident. The risk of rushing should be weighed as carefully as the risk of standing still. Regardless of the direction chosen, success potentials are increasing year over year. For example, in 2015, if one were to pose these realities in a debate, we might have been asking ourselves, "who's going to take the first hit by prematurely experimenting with this technology?" We might have been hard-pressed to find a volunteer. Now, we know who took the punch. Estonia. Almost immediately after Russia hacked them, they sought supranational intervention, thus inspiring conceptions of a new safety net to mitigate risk for alternative voting platforms: supranational brokerage.

Thus, the dilemma is not defining the problem (tabulation errors) but identifying what should be done. Some imply urgency for any step to be taken (such as Abdollah, who recognized in 2019 that the current operating system would soon expire). Others simply acknowledge that everything we do is experimentation (Beedham, 2018; Frost, 2022; Polyakov, 2022). Some advocate openly for integrating blockchain into electoral tabulation mechanisms (Gonzales et al., 2022; Hassan et al., 2022). Likewise, an equal number of qualified individuals argue the opposite— that blockchain e-voting systems are either too risky and too early to implement or simply that e-voting systems are insecure regardless of the base

technology (Park et al., 2022).

This project aims to present these inevitable policy puzzles without undercutting their complexity. Regarding policy and developing norms, will we see greater engagement with supranational security-backers like NATO, or will governments exploit them? Likewise, from a technological perspective, what opportunities and barriers do we encounter when considering applying this to larger-scale real-world contexts? In time, should a blockchain-based alternative outperform contemporary designs in all metrics mentioned above (accuracy, anonymity, scalability, and speed), their roles could reverse. In this case, the blockchain-based system would be the primary and the original a secondary verifier. Over time, the blockchain-based system may overtake the tabulation process entirely. Ultimately, we expect that a blockchain-based parallel electoral verification system is feasible. However, there are still blind spots in the hardware manufacturing process, ethical concerns, legal vacuums, and funding hurdles that need to be overcome before larger scaled models can be tested or implemented. Do the benefits of integrating this new technology outweigh the pros and cons of staying the same? It's a pick your poison dilemma.

CHAPTER 6

POLICY DEVELOPMENT PARADIGMS

Suppose we pause for a moment and recall what we've covered thus far. Throughout the manuscript, we've discussed the crisis of voting systems and the importance of standardized cybersecurity frameworks (such as the CSF Electoral Infrastructure Profile) in harmonizing future security strategies and objectives (Chapter 1). From here, we jumped into a historical overview (Chapter 2) of voting technology from ancient Greek ceramic shards to the present hybrid voting system (a mix of traditional paper ballots and e-voting options). The data vulnerabilities of e-voting (concerning the final voting and tabulation phases of electoral security frameworks) reflect in today's scholarly debate (Chapter 3). Should policies pursue blockchain-centric e-voting alternatives, reinforce the existing framework, or both? Though the dialogue can be described as multifaceted— technical, practical, policy-minded, and comparative— above all, it is polarized. One camp argues in favor of implementing blockchain-based e-voting alternatives, and the other is staunchly opposed. Walking through these opposing stances helps us frame, from a technical analytic rather than theoretical perspective, how blockchain could function in an election setting, either parallel to (or instead of) current tabulation systems. This naturally introduces us to the five global case studies in action (Chapter 4). Now, after outlining the risks and opportunity costs associated with these nascent technologies (Chapter 5) with respect to cybersecurity and electoral security frameworks (Chapter 1), we must ask ourselves: how should we move forward (Chapter 6)?

It would be dangerous to suggest that this technology be implemented in every (if any) political setting. As some scholars of decentralized justice noted, "the

power of technology to resolve disputes is exceeded by the power of technology to generate disputes" (Katsh and Robinovish-Einy, 2021). Though online dispute resolution (ODR) is growing, that it's still limited is a valid reason to slow the implementation of blockchain e-voting systems and, perhaps, focus on dispute resolution mechanisms first. However, in practice, legal precedents often develop in tandem when technology tests social boundaries — such as the litigation litter trailing behind Voatz, the most alarming pilot project worldwide at this moment.

Further, it's not illogical to surmise that the blockchain-based e-voting systems presented here are *not* viable for countries with institutional stability below a certain threshold. In both scenarios, implementing too early (i.e., introducing technological infrastructure without a management model or legal protections) could lead to rushed developments that decrease security and increase voter risk over protection. It would be nothing short of a disaster. Though this overview does *not* yield a clear way forward regarding whether blockchain-based e-voting initiatives should be pursued, this manuscript highlights some "red flags" and "green flags." These cases are among the first of their kind, but we can already see optimistic or worrying trends emerging from their respective technological ecosystems.

For example, in Estonia, arguably the biggest takeaway is that international backing is pivotal to thwarting external threats (such as the Russian hack). Supranational brokerage might function as a successful risk mitigator. This case inspires further investigation on the prospects of supranational brokerage with global governance institutions such as NATO (as Estonia did), the United Nations, the European Union, and the Internet Corporation for Assigned Names and Numbers (ICANN). The latter is perhaps one of the most hidden-in-plain-sight power players in the tech-driven world. ICANN is responsible for the infrastructural existence of

the internet and coordinating international policies and regulations through an organizational structure mirroring the UN and diplomatically engaging with world leaders to jurisdict internet provision in their country. They are immensely powerful in any country or region that relies on internet, yet they are virtually unheard of outside the field. It is also entirely possible some policies may reflect global asymmetries due to dealings with certain leaders regarding censorship, information provision, and other algorithmic elements. Nonetheless, it is an institution that may play a key role in policymaking regarding blockchain-based e-voting systems and, in particular, equalizing access.

From Russia, we can find several lessons. The first is that administrative unwillingness to address certain issues can compromise the system to dangerous levels despite the best efforts of the developers working on the project. Second, knowledge sharing and dispersion (such as Georgia's use of the Russian Exonum framework in certain administrative activities) can follow existing geopolitical rivers and create new ones. We might note the power of such actor-network relationships in defining international partnerships. For example, it's probable that the Palo-Alto partnership between the co-founders of ChainLink (Juan Bennet and Sergey Nazarov) introduced, at minimum, the auditing structure (Polyakov, 2022). If that is the case, it illustrates a clear example of how a "zone of expertise" (as opposed to the conception of a "liberal zone of peace") could cross-cut national boundaries (Doyle, 1983). Where this concept hits a wall is that issues pointed out in the system after two rounds of audits went unaddressed. Lack of follow-through may indicate either a development ceiling, dry funding, or that a complete strategic shift is in the works.

The case of Switzerland demonstrates a new strategy that moves away from task-centric infrastructure (focusing only on one use-case—elections) rather than

redefining the fundamental infrastructure (data management systems bureaucracies use to organize their citizens). They've shown that doing due diligence on the integrity of these broader data management systems can yield phenomenal results. Here, we see a clear emphasis on data management via a portal protecting citizens' personal data from ever being encrypted on-chain. The uPort portal translates their ID into a proxy that 'engages' with the chain. The portal strategy is a win-win way of protecting citizens and increasing the efficiency of national data management without imposing security sacrifices on the part of the government. The biggest question mark surrounding the Swiss case is the aspirations to extend that data system to interactions as minuscule as bike rentals and other small tasks. At what point in daily life does a citizen disengage from their ID, even if it's a proxy?

In Japan, the UniLayer-based smart city concept echoes the multi-functionality of the Swiss uPort and the designated registry system of Estonia. Likewise, we also notice some elements of design-in-use theory. By focusing on the umbrella concept of data management, both Japan and Switzerland are more flexibly and safely exploring ways to use smart contract protocols for extreme multi-functionality beyond what the original blockchain designers envisioned (alternative fin-tech). From its outset, the "Swiss Army Knife" system is structured to accommodate a wide set of administrative activities without compromising the data of the citizens registered on the chain.

Lastly, the legal tantrum thrown by the American-made Voatz illustrates the dangers of making the same mistake twice — allowing corporate entities without better security backgrounds to retrospectively fit a profit-seeking model to a sensitive security issue. This is not to say that there is no role for the private sector in this process, but corporate interest should not be allowed to bully the legal system into

catering to its needs, particularly when the stakes are so high. For example, when we look at major corporations (such as Overstock) backing private platforms (they own 10% of Voatz shares) or the political weight of individuals showing significant support (i.e., such as Bradley Tusk using his influence to mitigate a security PR scandal), do we view this as an entrepreneurial necessity or worry about their role in the future development of the platforms? Likewise, where a platform receives its initial launch funding and the business model describing its sustainability also plays a role in the ongoing success (or failure) of the platform.

Voatz also displayed a hesitancy to engage with external resources and delayed cooperation with the U.S. Department of Defense (DoD). Estonia had deeper veins of cooperation with the U.S. DoD via NATO collaboration than Voatz until the MIT researchers reported them. After multiple attempted hacks, Voatz expressed a preference that the hackers do not intervene unless working with an authorized bug bounty program (Amicus Curiae, 2020). Though well-versed legally, the bigger problem is not that lightweight hackers were successful (they weren't) but that they could get close enough. The Voatz platform, in its current form, *can* be compromised (Specter, 2021). Whether this emanates from a lack of transparency and corporate priorities outpacing security goals is unclear. However, Voatz presents a nightmare scenario for cybersecurity professionals (Weiss, 2019). Yet, because of political enthusiasm and monopoly, there is a high risk that recent history (the early 2000s to 2015) may repeat itself. When political rhetoric harkened for increased participation, rushing to adopt new EVM tech with significant vulnerabilities was less questioned. In 2002, the United States rushed to adopt an insecure voting mechanism; it is at risk of doing so again.

In the U.S. today, political decision-makers are trusting too much and not

asking enough questions. This runs precisely opposite of the general crypto ethos to 'trust less, verify more.' As the adage goes, "we forget our past, but embody all of it" (Updike, 1995).

Whether countries choose to fortify vulnerabilities in the current system or pursue blockchain e-voting alternatives (with their own set of risks) will have long-term consequences. What vulnerabilities we allow could feasibly determine, or at least influence, future political stability or instability. If a blockchain alternative is selected, the type of chain affects what self-sustaining funding options might be available. Almost all (if not all) of the chain cases discussed featured some form of smart-contract system tied to a permissioned or consortium chain anchored to a public chain. Below is an excerpt from an article on how to fund a permissioned (either hybrid or consortium) blockchain for supply-chain purposes:

> "In determining how to customize the funding structure in a permissioned blockchain, it must be decided how fees will be allocated and charged for financing the creation and validation operations as well as for the labor performed by the central authority" (Wegryzn and Wang, 2021).

Thus, any chain implemented for tabulation purposes will likely be permissioned if it facilitates some aspect of public administration activities. In a public chain, where participants are voluntary and anyone can join, the energy and computing costs of running and maintaining the chain would be dispersed amongst the users via transaction fees (i.e., gas fees) each time a user requests to initiate a transaction. (These differ per chain).

It's essential to recognize an incentive difference between permissionless and permissioned chains. In the latter, all parties are not only known, but they might not (especially if they are citizens of a nation implementing a voting system from the

top-down) have a genuine say as to whether they would like to be users. Instead, they might simply follow instructions to download an app, cast their vote, and think no more of it. To cause the least disruption, permissioned chains lean *away* from dispersing operating costs in the form of per transaction gas fees. How they do so (e.g., the funding structure they implement) will differ according to the needs and functionality of that chain. How the operating costs are dispersed (between users, central administrators, and third parties with a vested interest) could significantly influence the degree of decentralization (and democratization) of the chain's evolution. The more costs are dispersed over user nodes, the safer it is for them— but "free systems" (to users, but central absorption of cost) are more politically marketable. An unassuming public is likely to make decisions that are *not i*n their best long-term interest if it means they will save a few cents in the next five minutes.

6.1 Additional considerations and cautions

It is worth noting that the five case studies mentioned are not the only pilot projects in action; they are the most integrated projects with the highest likelihood of full implementation. Therefore, from a forecasting standpoint, they are a first-priority policymaking concern. Nonetheless, a wide range of companies and industries are developing blockchain-based voting technology. Among the other blockchain e-voting platforms oriented toward U.S. Elections are Scytl, Clear Ballot, Votem, and SmartMatic. (The Voatz debacle contributes to legal precedents affecting each of these systems). Internationally, one might also note Polyas in Finland or Intelvote covering Canada and Nova Scotia. More localized platforms such as Democracy Earth Foundation's "Sovereign," which attempts to create a space for a referendum and conflict resolution between the Colombian government and the FARC, Election

Runner and Boulé, a commercial voting platform under development, have shown how flexibly these systems can be tailored to circumstantial need (Heilweil, 2017))

As these projects advance in their respective corners of the globe, policymakers and analysts must include a few technical as well as non-technical considerations. An 'ideal voting system' would consider the eligibility, integrity, audibility, end-to-end privacy preservation, data accountability, and correctability and function autonomously with no authorities needed (Zhang et al., 2018). (The strategies and specifications of the data security would also ideally match or exceed those outlined by the CSF Electoral Infrastructure Profile) (Brady et al., 2021). Non-technical considerations might include the legal and ethical dimensions of development, pilot project testing (pre-implementation), implementation, and beta-testing (post-implementation testing). For example, there is an understated complexity created by cross-cutting alliances wherein national identities and individual technological relationships do not fall beneath the same labels. Likewise, highly sensitive and nuanced socio-political and politico-economic dynamics influence these technological ecosystems. This, in turn, reflects in their own (technological) gravitational pull on the legal and political spheres they exist within.

One must also consider hypothetical scenario that, even if a safe and vetted e-voting system became available, who would instrumentalist the issue? It's likely this would threaten lobbies profiting from lucrative longterm contracts with existing EVM producers. The political pushback against it may be just as intense as the tech communities pull in favor of new systems. Although progress could be hastened by greater cooperation between Washington D.C. and Silicon Valley, in some ways, their tendency to oppose each other creates an in-built check-and-balance where neither tramples the will of the other. Nonetheless, even in an idealistic theoretical

scenario where the technological development was completely clean, the politics of adoptioning it would still be messy.

These interconnected dynamics implicitly mean that we cannot isolate technical feasibility from other factors affecting the platform's success — or failure. Through these respective cases, we've problematized the issue of intellectual property, transparency laws, privacy laws, corporate versus bureaucratic dynamics, friendly versus malicious hacking, bug bounty programs and intermediaries, supranational brokerage prospects, and financial modeling, among other abstract issues not directly related to functionality but social structure integration (Zhang et al., 2018). Finally, all cases illustrate the fundamental importance of routine auditing and (where possible) initiating authorized hacking arrangements.

Conceptually, we must also keep in mind that attempts to use blockchain to improve election security also invite a reorientation of how bureaucracies categorize their own citizens. Blockchain denotes a fundamental shift in the technical architecture of verification systems from client-server (linear) to P2P (spatial). The client-server model has been the backbone of internet information queries since the early 1990s. Yet, the increasing utility and safety of P2P networks (horizontally distributed nodes) to securitize information make alternative use-cases such as elections attractive. Because smart contract registry frameworks involve a server-side credential (a decentralized government-issued ID), this infrastructure can operate as a broader personal data management system. All standard security measures, such as those presented by the Cybersecurity Framework (CSF) Election Infrastructure Profile, are relevant. However, this verification style (P2P) has two implications: (1) it changes how the citizen is integrated and represented in the bureaucratic system, and (2) widespread data management dominates isolated tasks. This means voting is

one function within a broader data infrastructure; voting is not *the* function for which this personal data is collected. That leaves room for other public services to rely on the same data pool. We see these nuances built into the Swiss case study from its outset.

In contrast, we notice the reverse in the Estonian case, wherein the focus began with elections, and it was soon determined that X-Road was needed to manage the citizens' data. Nonetheless, the result is the same: the primacy of data management. For each case study, whether the citizens' personal data is 'safer' (according to current CSF standards) in the alternative blockchain e-voting system than via standard EVM or DRE voting machines must be assessed. Because no two systems have the same degree of risk and vulnerabilities, this makes a blanket policy impossible to declare. Some smart contracted systems, such as the Swiss uPort, have demonstrated they may be ready for upscaling. However, others could introduce more danger than safety. Thus, whether blockchain could improve electoral security is entirely circumstantial.

CHAPTER 7

CLOSING THOUGHTS

Let's revisit October 2020, a moment of division that drew all eyes to Capitol Hill. It doesn't take much creative license to imagine Trump as an insatiable character who thrives on rocking the boat. Still, it is fictitious nonetheless to dive into someone's persona, conjuring thoughts they might have had. I cannot read Trump's mind any more than he can read mine. Neither of our thoughts matter— particularly in this analysis, which is *systemic,* not individualistic. However, that fictitious anecdote that opened this analysis presents itself as a political photograph—calling attention to the gravity of what technical fails in our current system and how they manifest in society. Trump is not a magician, nor is his successor. Like all politicians, they are opportunists acting and reacting to their institutional environment, sometimes pushing against and sometimes being pushed by it.

Nonetheless, we find ourselves staring at possibly the first moment in U.S. History where certain (social, not administrative) demographics split not simply over the looming vote outcome but over whether to continue counting. In no previous election have the slogans "Stop the count" nor "every vote counts" been shouted at each other. There's ample argument for the notion that both groups are incorrect. Is it beneficial to throw one's hands up in surrender? No.

Conversely, does every vote count? Also, no. We'd like to think it does, but the simple truth is that when the tabulation system is as vulnerable as it is, we can expect that a certain percentage of those will be tampered with or canceled out by manipulated ballots. It is as naïve to think that "every vote counts" as it is ignorant to try jamming a wedge into the counting. From every angle, this crisis of trust in

institutions and peers alike has not only stirred chaos and confusion but also inspired security specialists, analysts, and scholars to dig deeper (Taş and Tanrıöver, 2021). Social unrest should not be the driving impetus for recounts or additional verification in an ideal system. Though this is the unfortunate point we have arrived at, this manuscript optimistically argues that we don't have to stay here.

Moreover, after reviewing the literature on the subject, it's clear that most experts agree something must be done to fortify tabulation. However, even amongst those who are actively in favor of exploring remote and unverifiable or electronic ballots, how to go about this is far more controversial. The literature is polarized from this point onward. Moreover, when discussing internet, mobile, or blockchain-based e-voting systems, another level of valid concerns emerge.

In our enthusiasm to find an alternative, might we go from 'bad to worse' as some scholars fear? Hypothetically speaking, even if the new e-voting system *were* airtight, if it's implemented too soon, the legal system might be unprepared to handle potential disputes related to this uncharted technological territory. Worse, if the system that (ultimately) receives bureaucratic approval is a centralized abstraction of the original concept, citizen biometric information may be more vulnerable with lesser legal recourse than before. There is also the possibility that— as in the 100+ year delay in selecting and adopting basic mechanical and EVM technologies— even the best option might not yet be accepted at the appropriate moment making it nearly obsolete by the time decision-makers warm to it.

Fear, skepticism, resistance to change, bureaucratic bogs, legislative gaps, valid concerns, and information privacy concerns present legitimate obstacles. These factors are so significant that many might discourage exploring blockchain-based e-voting options at all. But to say so would be political equivalent to saying, "I attest

that placing national security in the guardianship of a Windows 7 operating system is a good idea….Any opposed?" Yes, nearly everyone is opposed. Not only is security porous, but the operating system contract extensio*n* expires in 2023— just before the 2024 U.S. presidential elections. There's a ticking two-year timebomb on the current tabulation system.

Institutional reform can act as a pressure valve. Updating EAC standards is step one, but a range of forward-thinking policies can prime for safe technological development practices (such creating more opportunities for friendly hackers or incentivize academic departments known to generate great thinkers, particularly the controversial ones, with the promise of jobs in national security).

While these issues are being troubleshot, tangible steps should be taken to prime the way for blockchain-based e-voting systems to be released safely. Number one, competition should be encouraged amongst emerging producers to avoid repeating the oligarchic pattern of the current EVM manufacturers. Likewise, cybersecurity specialists should have greater weight in selecting these platforms than under-qualified businesspeople and lobbyists. Likewise, the principles of subsidiarity should continue to be respected where possible.

One way of respecting this philosophy would allow municipal registries responsible for containing voter information can be segmented and localized offline. In addition, tiered verifications would mean that one's federal identity (a proxy of the individual's personal data) would still allow the citizen to participate in federal elections and other civic duties without compromising or exposing their personal data. This works in favor of national security as well because it makes sensitive citizen data less vulnerable to mass manipulation or external intervention (Taş and Tanrıöver, 2021).

In other words, it would be unwise to have one gigantic database responsible for universally protecting the complete information of all citizens of the country. Rather, a web of the county and state verification platforms can conduct the counts independently and report to a national (centralized) database afterward. This would also diversify pressure points for external intervention. It's not beneficial to create a golden goose egg of high-stakes raw data; better to create 1,000 ruddy brown chicken egg databases and scatter them. Likewise, close monitoring of existing scaled experiments worldwide, such as in local elections in Switzerland, Japan, and other locations involving beta-blockchain e-voting systems, can offer positive insights over time. Likewise, several companies have already emerged as key players in the field. These local and regional projects create a space for emerging technologies to be tamed and optimized befor*e* being scaled up to accommodate large populations of voters safely.

Ironically, validating blockchain e-voting systems can only come with preemptively puncturing as many holes in the system as possible. Vulnerability and inefficiency shouldn't be shied away from; they should be identified and corrected. In this, bug bounty programs, routine audits, and system patching are invaluable to detect errors before a malicious entity does. By asking what should be done to reduce risk, the ideas presented here become actionable rather than simply descriptive.

For example, preemptively identifying legislation regarding biometric registry and data privacy laws can fortify future legal safeguards, and registry procedures while mitigating barriers to entry for users on the network while increasing the overall security of the platform. Throughout the manuscript, we've assessed pilot projects and municipal experimentations around the globe. Our central aim has been to extract lessons and strategies from each of the case studies reviewed

thus far to inform future policy recommendations, particularly those pertaining to cybersecurity.

Though uncertainties abound, what we can do is take stock of the various lessons emanating from these cases in action. However, there's one lesson that can be derived from all cases. Introducing blockchain-based e-voting is not a "proceed-at-all-costs" situation, nor is it a dilemma that should make us too paralyzed to approach problem-solving. We should move ahead methodically but be ready to troubleshoot the technical issues along with the ethical ones, not favoring one over the other. After significant testing and monitoring, perhaps vetted models could be upscaled to operate, not as a replacement for existing electoral systems but as a parallel verification system.

The primary vote-counting method would still be available, but this secondary, blockchain-based system would run alongside the existing mechanism. If the results match, social disputes over the count *should* lose some steam. Conversely, suppose the results do not align. In that case, this could yield an opportunity for institutions to be proactive in alleviating the situation (i.e., social conflict emanating from election cycles and waning trust) before it worsens further. Social conflict reduction is as much a goal of the project as national security and protecting voters.

We live in a world where archaic invasion tactics (see Iraq, Afghanistan, Crimea, Ukraine, etc.) have yet to expire while a new digital realm has opened a new genre of vulnerability in the national security systems. Voting is just one element of national infrastructure, albeit a crucial one. However, we know that the crisis of electoral institutions is not one restricted to any given election, country, or era. Instead, it is a perennial problem that has worsened, season over season, in electoral systems worldwide. That the rhythm of blockchain beta-testing mirrors past electoral

technology adoption patterns (e.g., pocketed local experimentation worldwide) may mean that policymakers don't have much time until these dilemmas are on their doorstep. As we've seen, the role of blockchain in cybersecurity remains to be seen, not just for elections but for other administrative activities as well. The crisis of voting systems may be the impetus for new personal data management systems in governance altogether (Pelt et al., 2020). As these dynamics unfold, policymakers will need to confront what security thresholds will define whether blockchain-based e-voting infrastructure can be implemented in live elections and at what scale.

This may involve updating the CSF Election Infrastructure Profile or drafting a complimentary document geared towards blockchain platforms. Whether it is safe to proceed or not, the seeping adoption of blockchain-based e-voting systems may be inevitable. Thus, the technical, legal, and ethical policy dilemmas discussed here should be considered preemptively — rather than in the tailwinds —of technological developments about to blow beyond it.

Despite the significant flaws in the current hybrid system (paper and EVM voting option), we must be careful not to jump out of the frying pan and into the fire by rushing into an alternative, no matter how much potential it wields. Although this technology can offer greater electoral security and more accurate representation if designed well, it can make citizens more vulnerable to their own governments if abused. Depending on the socio-political context of the country implementing these measures, blockchain e-voting may have the power to emancipate citizens from electoral insecurity or enslave them to their own data.

REFERENCES

Abdollah, T. (2019). *AP Exclusive: New election systems use vulnerable software*. AP NEWS. Retrieved 28 January 2022, from https://apnews.com/article/operating-systems-ap-top-news-voting-voting-machines-pennsylvania-e5e070c31f3c497fa9e6875f426ccde1.

About ACE —. Aceproject.org. (2022). Retrieved 8 January 2022, from https://aceproject.org/about-en/.

About the election fraud database. The Heritage Foundation. (2021). Retrieved 2 November 2021, from https://www.heritage.org/article/about-the-election-fraud-database.

Al Ahmad, M., Al-Saleh, A., & Al Masoud, F. (2018). Comparison between PoW and PoS systems of cryptocurrency. *Indonesian Journal Of Electrical Engineering And Computer Science*, *10*(3), 1251. https://doi.org/10.11591/ijeecs.v10.i3.pp1251-1256.

Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H., Pervez, Z., & Dahal, K. (2019). DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. *Applied Sciences*, *9*(15), 2953. https://doi.org/10.3390/app9152953.

Alessie, D., Sobolewski, M., & Vaccari, L. (2019). *Blockchain for digital government: An assessment of pioneering implementations in public services* [Ebook] (pp. 31-35). European Commission, Joint Research Centre (JRC), Digital Economy Unit (JRC/B6). Retrieved 26 February 2022, from https://ec.europa.eu/jrc.

Alvarez, R., Hall, T., & Hyde, S. (2009). *Election fraud*. [United States]: Brookings Institution Press.

Alvarez, R., Adams-Cohen, N., Kim, S., & Li, Y. (2020). *Securing American Elections: How Data-Driven Election Monitoring Can Improve Our Democracy* (Elements in Campaigns and Elections). Cambridge: Cambridge University Press. doi:10.1017/9781108887359

A new low for global democracy. (2022). Retrieved 24 April 2022, from https://www.economist.com/graphic-detail/2022/02/09/a-new-low-for-global-democracy.

Ansper, A., Buldas, A., Jürgenson, A., Oruaas, M., Priisalu, J., & Raiend, K. et al. (2010). *E-voting concept security: analysis and measures* [Report] (pp. 1-54). Estonian National Election Committee. Retrieved 8 February 2022, from http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf.

Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S., & AlSalman, H. et al. (2022). A liquid democracy enabled blockchain-based electronic voting system. *Scientific Programming*, *2022*, 1-10. https://doi.org/10.1155/2022/1383007.

Aouidef, Y., Ast, F., & Deffains, B. (2021). Decentralized justice: a comparative analysis of blockchain online dispute resolution projects. *Frontiers In Blockchain*, *4*. doi: 10.3389/fbloc.2021.564551

Asenbaum, H. (2018). Anonymity and democracy: absence as presence in the public sphere. *American Political Science Review, 112*(3), 459-472. doi:10.1017/S0003055418000163.

Aoussat, A., Buisine, S., & Nelson, J. Design in use: some methodological considerations, 1-5. Retrieved from http://stephanie.buisine.free.fr/publis/CIRP09.pdf.

Axelrod, R. (1984). *The evolution of cooperation*. New York: Basic Books.

Axelrod, R., & Keohane, R. (1985). Achieving Cooperation under Anarchy: Strategies and Institutions. *World Politics*, *38*(1), 226-254. doi: 10.2307/2010357.

Azcleanelections.gov, A. (2021). *How votes are counted | Citizens Clean Elections Commission (CCEC)*. Azcleanelections.gov. Retrieved 15 May 2021, from https://www.azcleanelections.gov/election-security/how-votes-are-counted.

Azpuru, D., & Hall, M. (2017). Retrieved 24 April 2022, from https://www.vanderbilt.edu/lapop/news/022317.US-WashingtonPost.pdf.

Azure Scheduler will be retired on 31 January 2022 | Azure updates | Microsoft Azure. Azure.microsoft.com. (2022). Retrieved 15 March 2022, from https://azure.microsoft.com/en-us/updates/azure-scheduler-will-be-retired-on-31-january-2022/.

Bardhan, P. (2021). *The two largest democracies in the world are the sickest now*. Scroll.in. Retrieved 2 November 2021, from https://scroll.in/article/971086/the-two-largest-democracies-in-the-world-are-the-sickest-now.

Beedham, M. (2018). *Japan is experimenting with a blockchain-powered voting system*. TNW | Hardfork. Retrieved 31 January 2022, from https://thenextweb.com/news/japan-city-blockchain-voting.

Bennet, J., Couture, S., & Crain, B. (2015). *EB100- Juan Benet: decentralizing the web with Interplanetary File Systems (IPFS)*. Youtube.com. Retrieved 27 February 2022, from https://www.youtube.com/watch?v=erB7i6Uc4DM.

Bennett, C., Bender, B., Scola, N., & Geller, E. (2016). *Hacker threat extends beyond parties*. Politico. Retrieved 17 March 2022, from https://www.politico.com/story/2016/07/elections-parties-hacking-226467;.

Blake, A. (2020). *Is Mac more secure than windows? We asked the experts | Digital Trends*. Digital Trends. Retrieved 28 January 2022, from https://www.digitaltrends.com/computing/privacy-macos-or-windows-we-asked-the-experts/.

Brady, M., Howell, G., Franklin, J., Sames, C., Schneider, M., Snyder, J., & Weitzel, D. (2021). *Cybersecurity framework election infrastructure profile* [Ebook] (pp. 1-82). National Institute of Standards and Technology - U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8310-draft.pdf.

Bueno de Mesquita, B., & Lalman, D. (1992). *War and Reason: Domestic and International Imperatives*. Yale University Press.

Casino, F., Dasaklis, T., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics And Informatics*, *36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.006.

Casey, W., J.A., J., & Mishra, B. (2016). Wireless mobile networks, ubiquitous computing, and dependable applications. *Threats from inside: dynamic utility (mis)alignments in an agent-based model*, *7*, 97117. Retrieved 9 February 2022.

Casey, W., Kellner, A., Memarmoshrefi, P., Morales, J., & Mishra, B. (2019). *Communications of the ACM*, *62*(1), 85-93. https://doi.org/10.1145/3190836.

Centierio, H. (2022). *A complete decoding of the bitcoin block*. Medium. Retrieved 8 February 2022, from https://levelup.gitconnected.com/a-complete-decoding-of-the-bitcoin-block-578904267142.

Çelebi, S. (2015). Civic engagement in Turkey's democracy: the case of "Oy ve Ötesi". *Turkish Policy Quarterly*, *13*(4), 71-78. Retrieved from http://turkishpolicy.com/files/articlepdf/civic-engagement-in-turkeys-democracy-the-case-of-oy-ve-otesi-winter-2015-en.pdf.

Chełkowski, T., Jemielniak, D., & Macikowski, K. (2021). Free and Open Source Software organizations: A large-scale analysis of code, comments, and commits frequency. *PLOS ONE*, *16*(9), e0257192. https://doi.org/10.1371/journal.pone.0257192.

Chuvakin, A., & Williams, B. (2010). *Disk encryption: data at rest*. Science Direct. Retrieved 28 January 2022, from https://www.sciencedirect.com/topics/computer-science/disk-encryption.

Cliffe, J. (2021). How strongmen cling to power. Retrieved 15 April 2022, from https://www.newstatesman.com/international-politics/democracy-international-politics/2021/11/how-strongmen-cling-to-power.

Crawford, T. (2020). Actor-Network Theory. *Oxford Research Encyclopedia Of Literature*. doi: 10.1093/acrefore/9780190201098.013.965.

Crypto Research, Data, and Tools. Messari.io. (2022). Retrieved 8 March 2022, from https://messari.io/asset/unilayer/profile.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Appl. Innovation*, *2*, 6-10. Retrieved 8 February 2022.

Crypto Valley Association. LinkedIn. (2022). Retrieved 26 February 2022, from https://www.linkedin.com/company/crypto-valley-association/?originalSubdomain=ch.

CSRC Topics - cybersecurity framework | CSRC. (2022). Retrieved 29 April 2022, from https://csrc.nist.gov/Topics/Applications/cybersecurity-framework.

Current status of the U.S. Engineering and Computing Workforce, 2019 – IRA | ASEE. Ira.asee.org. (2022). Retrieved 8 January 2022, from https://ira.asee.org/national-benchmark-reports/workforce2019/.

Coda | A new doc for teams.. Coda | A new doc for teams. (2022). Retrieved 9 February 2022, from https://coda.io/about.

Colatin, S. (2022). *Cyber attacks against Estonia (2007 Excerpt)*. International cyber law: interactive toolkit. *NATO Cooperative Cyber Defence Centre of Excellenc*e. Retrieved 8 February 2022, from https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007).

Cortés, E. (2017). *Testimony of Edgardo Cortés commissioner, Virginia department of elections* [Ebook] (pp. 1-5). House of Representatives. Retrieved 2 February 2022, from https://docs.house.gov/meetings/GO/GO25/20171129/106602/HHRG-115-GO25-Wstate-CrtesE-20171129.pdf.

Comparative Data —. Aceproject.org. (2022). Retrieved 8 January 2022, from https://aceproject.org/epic-en/CDTable?view=country&question=VR008.

Dandoy R. The impact of e-voting on turnout: insights from the Belgian case, 29–37. ISBN: 978-3-907589-17-5. DOI: 10.1109/ICEDEG.2014.6819940.

Davis, J., & Nast, C. (2007). *Hackers take down the most wired country in Europe*. Wired. Retrieved 8 February 2022, from https://www.wired.com/2007/08/ff-estonia/.

Definition of enterprise-grade - Gartner Information Technology Glossary. Gartner. (2022). Retrieved 7 February 2022, from https://www.gartner.com/en/information-technology/glossary/enterprise-grade.

Department of Defense press briefing by Secretary Carter and Gen. Dunford in the Pentagon. U.S. Department of Defense Briefing Transcript by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room. (2016). Retrieved March 22, 2022, from https://www.defense.gov/News/Transcripts/Transcript/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the/Â

Democracy Index 2020 - Economist Intelligence Unit. Economist Intelligence Unit. (2021). Retrieved 2 November 2021, from https://www.eiu.com/n/campaigns/democracy-index-2020/.

Democracy in Retreat. Freedom House. (2018). Retrieved 24 February 2022, from https://freedomhouse.org/report/freedom-world/2019/democracy-retreat.

Difference between client-server and peer-to-peer network - GeeksforGeeks. GeeksforGeeks. (2020). Retrieved 2 February 2022, from https://www.geeksforgeeks.org/difference-between-client-server-and-peer-to-peer-network/.

Doboli, A., & Umbarkar, A. (2014). The role of precedents in increasing creativity during iterative design of electronic embedded systems. *Design Studies, 35,* 298–326.

Doyle, M. (Summer 1983). Kant, liberal legacies, and foreign affairs. *Philosophy & Public Affairs*, *12*(3), 205-235.

Doyle, M. (Fall1983). Kant, liberal legacies, and foreign affairs, Part 2. *Philosophy & Public Affairs*, *12*(3), 323-353.

Dunn, P. (2016). Theories of technology and society – Peter T. Dunn. Retrieved 13 April 2022, from https://sites.uw.edu/ptdunn/stss/comm-tech-society/.

Dusek, V. (2006). *Philosophy of technology: an introduction*. Malden, MA: Blackwell.

Earle, G. (2021). *Trump's barrage of lawsuits where he is losing ground to Joe Biden*. Mail Online. Retrieved 15 May 2021, from https://www.dailymail.co.uk/news/article-8917907/Donald-Trumps-barrage-lawsuits-losing-ground-Joe-Biden-explained.html.

Economist Intelligence Unit (EUI). (2022). *Democracy Index 2021: The China Challenge* [Ebook] (pp. 12-16). Retrieved from https://pages.eiu.com/rs/753-RIQ-438/images/eiu-democracy-index-2021.pdf?mkt_tok=NzUzLVJJUS00MzgAAAGD8eEIpD3o2UZrUjPwvVaD56IoxB62daBPqBXeFmLv3eGWO4Is3zwtvLwHO1vkrpJ_cCQbmliqRoPtzniU1HDvpd-rCbvT82SigYYK7duFZGPeUw.

Electronic Voting | US House of Representatives: History, Art & Archives. History.house.gov. (2022). Retrieved 28 January 2022, from https://history.house.gov/Exhibitions-and-Publications/Electronic-Technology/Electronic-Voting/.

Engin, Z., & Treleaven, P. (2019). Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies. *The Computer Journal*, *62*(3), 448-460. doi: 10.1093/comjnl/bxy082.

Epstein, J. (2021). *Decertifying the worst voting machine in the US*. Freedom-to-tinker.com. Retrieved 2 November 2021, from https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/.

Epstein, R., Ember, S., Gabriel, T., & Baker, M. (2020). How the Iowa Caucuses Became an Epic Fiasco for Democrats (Published 2020). Retrieved 15 April 2022, from https://www.nytimes.com/2020/02/09/us/politics/iowa-democratic-caucuses.html.

Federal Council Report. (2018). *Legal framework for distributed leger technology and blockchain in Switzerland: an overview with a focus on the financial sector* (pp. 11-140). Geneva. Retrieved from https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

Feenberg, A. (2017). *Technosystem: the social life of reason*. Cambridge, MA and London: Harvard University Press.

Finnish immigration service & MONI | PositiveBlockchain.io. PositiveBlockchain.io. (2022). Retrieved 9 February 2022, from https://positiveblockchain.io/database/finnish-immigration-service-moni/.

Frankenfield, J., & Rasure, E. (2021). *Gas (Ethereum)*. Investopedia. Retrieved 8 March 2022, from https://www.investopedia.com/terms/g/gas-ethereum.asp.

Frost, L. (2022). Moscow to use blockchain voting for changes to Russia's Constitution. Decrypt. Retrieved 14 February 2022, from https://decrypt.co/31413/moscow-to-use-blockchain-voting-for-changes-to-russias-constitution.

Gan, Q., Lau, R., & Hong, J. (2021). A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach. *Technology Analysis & Strategic Management*, 1-17. https://doi.org/10.1080/09537325.2021.1979509.

Germann M , Serdült U. Internet voting and turnout: evidence from Switzerland. *Elect Stud* 2017;47:1–12.

Gilbert H., Handschuh H. (2004) Security Analysis of SHA-256 and Sisters. In: Matsui M., Zuccherato R.J. (eds) Selected Areas in Cryptography. SAC 2003. Lecture Notes in Computer Science, vol 3006. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24654-1_13.

Grieco, J. (1988). Realist Theory and the Problem of International Cooperation: Analysis with an Amended Prisoner's Dilemma Model. *The Journal Of Politics*, *50*(3), 600-624. doi: 10.2307/2131460.

Goodman N , Stokes LC. Reducing the cost of voting: an evaluation of internet voting's effect on turnout. Br J Polit Sci 2020;50:1155–67.

Gorenflo, C., Lee, S., Golab, L, Keshav, S. (2020) FastFabric: Scaling Hyperledger Fabric (HF) to 20,000 transactions per second. *Int. J. Netw. Manag:* 30.

González, C., Mena, D., Muñoz, A., Rojas, O., & Sosa-Gómez, G. (2022). A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Hindawi Applied Sciences*, *12*, 1-14. https://doi.org/https://doi.org/10.3390/app12020531

Greenberg, A. (2016, March 2). *Pentagon launches the Feds' first 'bug bounty' for Hackers*. Wired. Retrieved March 22, 2022, from https://www.wired.com/2016/03/pentagon-launches-feds-first-bug-bounty-hackers/

Hallström, J. (2020). Embodying the past, designing the future: technological determinism reconsidered in technology education. *International Journal Of Technology And Design Education*, *32*(1), 17-31. doi: 10.1007/s10798-020-09600-2.

Heilweil, R. (2022). Nine companies that want to revolutionize voting technology. Retrieved 30 April 2022, from https://www.forbes.com/sites/rebeccaheilweil1/2017/12/02/eight-companies-that-want-to-revolutionize-voting-technology/?sh=79edd5b712c1.

Home | ethereum.org. ethereum.org. (2022). Retrieved 9 February 2022, from https://ethereum.org/en/.

How Aung San Suu Kyi sees the Rohingya crisis. BBC News. (2018). Retrieved 15 May 2021, from https://www.bbc.com/news/world-asia-42824778.

How does AES-256 encryption work to protect your data. Atpinc.com. (2019). Retrieved 28 January 2022, from https://www.atpinc.com/blog/what-is-aes-256-encryption.

How Uniswap works | Uniswap. Docs.uniswap.org. (2022). Retrieved 8 March 2022, from https://docs.uniswap.org/protocol/V2/concepts/protocol-overview/how-uniswap-works.

Internet Voting in Estonia. (2022). Retrieved 15 April 2022, from https://www.ndi.org/e-voting-guide/examples/internet-voting-in-estonia.

InterPlanetary File System - GeeksforGeeks. GeeksforGeeks. (2022). Retrieved 27 February 2022, from https://www.geeksforgeeks.org/interplanetary-file-system/.

IPFS Powers the distributed web. Ipfs.io. (2022). Retrieved 27 February 2022, from https://ipfs.io.

Jafar, U., Aziz, M., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. *Sensors*, *21*(17), 5874. https://doi.org/10.3390/s21175874.

Jakobsson, M., & Juels, A. (1999). Proofs of work and bread pudding protocols (Extended Abstract). *Secure Information Networks*, 258-272. https://doi.org/10.1007/978-0-387-35568-9_18.

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167-214. doi: 10.2307/2009958.

Jiji. (2018). *LayerX will develop blockchain-based voting system using digital ID verification in Japan*. The Japan Times: Independent Voice of Asia. Retrieved 7 March 2022, from https://www.citethisforme.com/cite/sources/websiteautociteconfirm.

Juskalian, R. (2018). *Inside the Jordan refugee camp that runs on blockchain*. MIT Technology Review. Retrieved 9 February 2022, from https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.

Karsev, A. (2022). *Best and worst of ICO gold rush: how technology created a market and greed doomed it | CoinMarketCap*. CoinMarketCap Alexandria. Retrieved 11 March 2022, from https://coinmarketcap.com/alexandria/article/best-and-worst-of-ico-gold-rush-how-technology-created-a-market-and-greed-doomed-it.

Keohane, R., & Nye Jr., J. (1989). *Power and interdependence: world politics in Transition* (3rd ed., pp. ch. 1-2: 3-32). Boston: Little-Brown.

Kim, S. (2020). What to know about Shadow Inc., the vendor behind Iowa Democrats' caucus app. Retrieved 15 April 2022, from https://abcnews.go.com/Politics/shadow-vendor-iowa-dems-reporting-app/story?id=68754002.

Kwatra, K. (2022). *What is IPFS?*. Medium. Retrieved 27 February 2022, from https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5.

Kalvet, T., Tiits, M., & Hinsberg, H. (eds.). (2013). Effectiveness and impact of using e-services. Tallinn: Baltic Research Institute and Center for Policy Studies Praxis.

Khan, S., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-To-Peer Networking And Applications*, *14*(5), 2901-2925. https://doi.org/10.1007/s12083-021-01127-0.

King, E. (2016, updated 2020). *How the U.S. ended up with today's paper ballots*. Time. Retrieved 15 May 2021, from https://time.com/4305508/paper-ballot-history/.

Klebnikov, S. (2022). Russian government resigns as Putin proposes changes to the constitution. Forbes. Retrieved 25 February 2022, from https://www.forbes.com/sites/sergeiklebnikov/2020/01/15/russian-government-resigns-amid-putins-proposed-changes-to-the-constitution/?sh=119817cb5ec7.

Kosmin, P. (2015). A phenomenology of democracy. *Classical Antiquity*, *34*(1), 121-162. https://doi.org/10.1525/ca.2015.34.1.121.

Kunda, Z. (1990). "The case for motivated reasoning." Psychological Bulletin. 108(3): 480-498. Doi:10.1037/0033-2909.108.3.480.

Kotz, D. (2008). Neoliberalism and financialization, 1-20. Retrieved from https://people.umass.edu/dmkotz/Neolib_and_Fin_08_03.pdf.

Lay, R. (2022). *The Philippines looks to blockchain voting for its diaspora*. Forkast. Retrieved 10 February 2022, from https://forkast.news/philippines-blockchain-voting-voatz.

LayerX - Headquarter Locations, Competitors, Financials, Employees. Cbinsights.com. (2022). Retrieved 8 March 2022, from https://www.cbinsights.com/company/layerx.

LayerX will develop blockchain-based voting system using digital ID verification in Japan. Cointelegraph: The Future of Money. (2020). Retrieved 7 March 2022, from https://cointelegraph.com/news/layerx-will-develop-blockchain-based-voting-system-using-digital-id-verification-in-japan.

Lee, T. (2022). Online voting vendor Voatz urges Supreme Court to limit security research. Retrieved 15 April 2022, from https://arstechnica.com/tech-policy/2020/09/online-voting-vendor-voatz-urges-supreme-court-to-limit-security-research/.

Lien, T., Bennett, B., Dave, P., & Queally, J. (2016). *Apple CEO says helping FBI hack into terrorist's iPhone would be 'too dangerous'*. Los Angeles Times. Retrieved 18 February 2022, from https://www.latimes.com/local/lanow/la-me-apple-san-bernardino-terror-20160218-story.html.

Linux Foundation - Decentralized innovation, built with trust. Linux Foundation. (2022). Retrieved 9 February 2022, from https://www.linuxfoundation.org/?sscid=CjwKCAjw2P-KBhByEiwADBYWCn_flYF0OgavXnv-aita0sQzVKsERJHSbZpGLa2u2SYa1z2DRYtMexoCuK8QAvD_BwE&gclid=CjwKCAjw2P-KBhByEiwADBYWCn_flYF0OgavXnv-aita0sQzVKsERJHSbZpGLa2u2SYa1z2DRYtMexoCuK8QAvD_BwE.

Lee Rainie, K. Scott, A. Perrin. *Americans' trust in government, each other, leaders*. Pew Research Center - U.S. Politics & Policy. (2019). Retrieved 7 January 2022, from https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/.

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal Of Cybersecurity*, *3*(2), 81-90. doi: 10.1093/cybsec/tyx008.

Martinson, P. (2019). *Estonia- the digital republic secured by blockchain* [Ebook] (pp. 1-11). Aktsiaselts PriceWaterhouseCoopers (PWC). Retrieved 10 February 2022, from https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.

McQuaid, D. (2022). ETH 2.0: What's happened so far and when is the next phase?. Currency.com. Retrieved 15 March 2022, from https://currency.com/eth-2-0-what-s-happened-so-far-and-when-is-the-next-phase.

Meyer, D. (2018). Blockchain voting notches another success—This Time in Switzerland. Fortune. Retrieved 26 February 2022, from https://fortune.com/2018/07/03/blockchain-voting-trial-zug/.

Miller, B. (2022). *West Virginia becomes first state to test mobile voting by blockchain in a federal election*. GovTech. Retrieved 10 February 2022, from https://www.govtech.com/biz/west-virginia-becomes-first-state-to-test-mobile-voting-by-blockchain-in-a-federal-election.html.

Moore, N. (2016). *U-M researchers put musical signature on hack into D.C. voting test*. Ur.umich.edu. Retrieved 17 March 2022, from https://www.ur.umich.edu/update/archives/101008/dchack.

MSRC - Microsoft Security Response Center. Technet.microsoft.com. (2021). Retrieved 2 November 2021, from https://technet.microsoft.com/en-us/library/security/ms04-011.aspx.

Nast, C. (2022). Amid war with Apple, the feds buddy up to Silicon Valley. Retrieved 15 April 2022, from https://www.wired.com/2016/03/defense-secretary-carter-gov-silicon-valley-team/.

Nast, C. (2022). Pentagon launches the feds' first 'bug bounty' for hackers. Retrieved 15 April 2022, from https://www.wired.com/2016/03/pentagon-launches-feds-first-bug-bounty-hackers/.

National cyber security audit summary. Voatz.com. (2022). Retrieved 15 March 2022, from https://voatz.com/wp-content/uploads/2020/07/NCC-Audit-Summary-Utah-County-Primary-Election-2019-Final.pdf.

New York Times Profiles Voatz. (2022). Retrieved 15 April 2022, from https://www.prnewswire.com/news-releases/new-york-times-profiles-voatz-301004581.html.

Nevada Voting Information. (2022). Retrieved 9 May 2022, from https://www.vote411.org/nevada.

Norris, P. (2018). Electoral integrity in America — Pippa Norris. Retrieved 28 April 2022, from https://www.pippanorris.com/electoralintegrityinamerica.

Norris, P. (2020). *Election integrity in the 2020 U.S. elections* [Report] (pp. 4-23). Harvard Kennedy School. Retrieved 8 February 2022, from http://www.electoralintegrityproject.com.

Norris, P., & Grömping, M. (2019). Perceptions of electoral integrity, (PEI-7.0). *Harvard Dataverse*, *2*(7). https://doi.org/Norris, Pippa; Grömping, Max, 2019, "Perceptions of Electoral Integrity, (PEI-7.0)", https://doi.org/10.7910/DVN/PDYRWL, Harvard Dataverse, V2, UNF:6:2wnukYraCZzg+gojPE/Ijg== [fileUNF]

Norden, L., & Beard, A. (2022). *There is shockingly little oversight of private companies that create voting technologies*. Brennan Center for Justice. Retrieved 8 January 2022, from https://www.brennancenter.org/our-work/analysis-opinion/there-shockingly-little-oversight-private-companies-create-voting.

Oneal, J., Oneal, F., Maoz, Z., & Russet, B. (1996). The liberal peace: interdependence, democracy, and international conflict 1950-85. *Sage*, *33*(1), 11-28. Retrieved from https://www.jstor.org/stable/425131.

O'Reilly, T. (2022). Open data and algorithmic regulation. Retrieved 15 April 2022, from https://beyondtransparency.org/chapters/part-5/open-data-and-algorithmic-regulation/.

Orr, G. (2016). *Elections as rituals: private, communal and public – Parliament of Australia*. Aph.gov.au. Retrieved 27 January 2022, from https://www.aph.gov.au/About_Parliament/Senate/Powers_practice_n_procedures/pops/Papers_on_Parliament_66/Elections_as_Rituals_-_Private_Communal_and_Public.

Óskarsdóttir, M., & Mallett, J. (2021). Strangely mined bitcoins: empirical analysis of anomalies in the bitcoin blockchain transaction network. *PLOS ONE*, *16*(9), e0258001. doi: 10.1371/journal.pone.0258001.

Ottis, R. (2007). *Analysis of the 2007 cyber attacks against Estonia from the fnformation warfare perspective* [Ebook] (pp. 1-6). Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDOE). Retrieved from https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Park, S., Specter, M., Narula, N., & Rivest, R. (2021). Going from bad to worse: from Internet voting to blockchain voting. *Journal Of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyaa025.

Paul LeBlanc, C. (2021). *Federal authorities expected to erect 'non-scalable' fence around White House*. CNN. Retrieved 15 May 2021, from https://edition.cnn.com/2020/11/02/politics/white-house-fence-erected-again/index.html.

Persily, N. (2017). Can democracy survive the internet?. *Journal Of Democracy*, *28*(2), 63-76. doi: 10.1353/jod.2017.0025.

Pelt, R., Jansen, S., Baars, D., & Overbeek, S. (2020). Defining blockchain governance: a framework for analysis and comparison. *Information Systems Management*, *38*(1), 21-41. https://doi.org/10.1080/10580530.2020.1720046.

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, *7*(2), 229-233. https://doi.org/10.1016/j.icte.2020.09.002.

Polachek, S. (1980). Conflict and trade. *Journal Of Conflict Resolution*, *24*(1), 55-78. doi: 10.1177/002200278002400103.

Polyas. (2022). Case studies about online voting. Retrieved 3 May 2022, from https://www.polyas.com/case-studies.

Powell, W. (1990). Neither market nor hierarchy: new forms of organization. *Research In Organizational Behavior*, *12*(1-55938-029-2), 295-336. Retrieved from https://pdodds.w3.uvm.edu/files/papers/others/1990/powell1990a.pdf.

Prakash, A., Satish, M., Bhargav, T., & Bhalaji, N. (2016). Detection and mitigation of denial-of-service attacks using stratified architecture. *Procedia Computer Science*, *87*, 275-280. https://doi.org/10.1016/j.procs.2016.05.161.

Pennsylvania Department of the Auditor General-Auditor General DePasquale: Officials in 18 counties report accepting gifts from voting equipment vendors. Paauditor.gov. (2022). Retrieved 8 January 2022, from https://www.paauditor.gov/press-releases/auditor-general-depasquale-officials-in-18-counties-report-accepting-gifts-from-voting-equipment-vendors.

Polyakov, K. (2022). How Moscow organized voting on blockchain in 2020. Ict.moscow. Retrieved 9 February 2022, from https://ict.moscow/en/news/how-moscow-organized-voting-on-blockchain-in-2020/.

Quorum - Public Affairs Software. (2022). Retrieved 9 February 2022, from https://www.quorum.us.

Racsko, P. (2019). Blockchain and democracy. *Society And Economy*, *41*(3), 353-369. doi: 10.1556/204.2019.007.

Raval, S. (2017). *An introduction to the interplanetary file system*. Youtube.com. Retrieved 27 February 2022, from https://www.youtube.com/watch?v=BA2rHlbB5i0.

Registered Manufacturers | U.S. Election Assistance Commission. (2022). Retrieved 15 April 2022, from https://www.eac.gov/voting-equipment/registered-manufacturers.

Ria Novosti. *В ЦИК объяснили сбой в работе сайта для электронного голосования*. РИА Новости. (2022). Retrieved 14 February 2022, from https://ria.ru/20200625/1573451457.html.

Ricardo, D., Sraffa, P., & Dobb, M. (1817). *On the principles of political economy and taxation* (pp. 160-162).

Rinkeby | Anyblock Analytics. Anyblock Analytics. (2022). Retrieved 26 February 2022, from https://www.anyblockanalytics.com/networks/ethereum/rinkeby/.

Robert Strauss Center for International Security and Law. (2013). *Elections and social conflict in Africa* (pp. 1-7). Austin, Texas: CCAPS: Climate Change and African Political Stability. Retrieved from https://www.files.ethz.ch/isn/161758/CCAPS%20Research%20Brief%20No.%206_final.pdf.

Role of the states in regulating federal elections | Constitution Annotated | Congress.gov | Library of Congress. Constitution.congress.gov. (2021). Retrieved 15 May 2021, from https://constitution.congress.gov/browse/essay/artI_S4_C1_1_1_1_1/.

Rosenberg, M. (2020). *Voting on your phone: new elections app ignites security Debate (Published 2020)*. Nytimes.com. Retrieved 17 March 2022, from https://www.nytimes.com/2020/02/13/us/politics/voting-smartphone-app.html.

Rosenberg, M., Corasaniti, N., Frenkel, S., & Perlroth, N. (2020, February 4). *Faulty Iowa app was part of push to restore Democrats' digital edge*. The New York Times. Retrieved March 25, 2022, from https://www.nytimes.com/2020/02/04/us/politics/iowa-caucus-shadow-app.html.

Rotondi, J. (2022). *Vote-by-Mail programs date back to the Civil War*. HISTORY. Retrieved 8 February 2022, from https://www.history.com/news/vote-by-mail-soldiers-war.

Russian government resigns. TASS. (2020). Retrieved 25 February 2022, from https://tass.com/politics/1109047.

Salehyan, I., & Linebarger, C. (2014). Elections and social conflict in Africa, 1990–2009. *Studies In Comparative International Development*, *50*(1), 23-49. https://doi.org/10.1007/s12116-014-9163-1

Schneier, B. (2004). *Essays: what's wrong with electronic voting machines? - Schneier on Security*. Schneier.com. Retrieved 27 October 2021, from https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html.

Schneier, B. (2020). Voatz internet voting app is insecure. Retrieved 15 April 2022, from https://noise.getoto.net/2020/02/17/voatz-internet-voting-app-is-insecure/.

Security Council unity 'crucial' to support democracy in Myanmar. UN News. (2022). Retrieved 27 January 2022, from https://news.un.org/en/story/2021/02/1083622.

Segal, A. (2017). Bridging the cyberspace gap - Washington and Silicon Valley. *Prism: The Journal of Complex Operations*, *7*(2). Retrieved from https://cco.ndu.edu/PRISM-7-2/Article/1401912/bridging-the-cyberspace-gap-washington-and-silicon-valley/.

Segal, A. (2017). Rebuilding Trust Between Silicon Valley and Washington. Retrieved 30 April 2022, from https://www.cfr.org/report/rebuilding-trust-between-silicon-valley-and-washington.

Seth, S. (2021). *Public, private, permissioned blockchains compared*. Investopedia. Retrieved 9 February 2022, from https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

Serdült, U., Germann, M., Harris, M., & Tambouris, E., et al. (2015). *Electronic Government and Electronic Participation.* Innovation and the Public Sector. (1st ed., pp. 27-41). The Netherlands: IOS Press. ISBN: 9781614995692. DOI: 10.3233/978-1-61499-570-8-27.

Shovkhalov, S., & Idrisov, H. (2021). Economic and legal analysis of cryptocurrency: scientific views from Russia and the Muslim world. *Laws*, *10*(2), 32. https://doi.org/10.3390/laws10020032.

Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations*.

Smith, Z. (2022). *Apple becomes 1st company worth $3 Trillion—greater than the GDP of the UK*. Forbes. Retrieved 24 February 2022, from https://www.forbes.com/sites/zacharysmith/2022/01/03/apple-becomes-1st-company-worth-3-trillion-greater-than-the-gdp-of-the-uk/?sh=78178eec5603.

Specter, M., Koppel, J., & Weitzer, D. (2021). The ballot is busted before the blockchain: a security analysis of Voatz, the first internet voting application used in U.S. federal elections. *Internet Policy MIT*, 1-19. Retrieved 11 March 2022, from https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf.

Spirakis, G., Spiraki, C., & Nikolopoulos, K. (2010). The impact of electronic government on democracy: e-democracy through e-participation. *Electronic Government, An International Journal*, *7*(1), 75. https://doi.org/10.1504/eg.2010.029892

Stewart K , Taylor J. *Online voting: the solution to declining political engagement?*, 2018. https://www.rand.org/blog/2018/03/online-voting-the-solution-to-declining-political-engagement.html [https://perma.cc/DTY4-F54U] (6 January 2021, date last accessed).

Stoddard, M., Garber, L., Merloe, P., Cowan, G., Wollack, K., Hennessey, J., & George, S. (1995). *How domestic organizations monitor elections* [Ebook]. National Democratic Institute (NDI) for International Affairs. Retrieved from https://www.ndi.org/sites/default/files/Domestic-Election-Monitoring-AtoZ-ENG.pdf.

Switzerland's first municipal blockchain vote hailed a success. SWI swissinfo.ch. (2018). Retrieved 31 January 2022, from https://www.swissinfo.ch/eng/crypto-valley-_-switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928.

Syed, I. (2022). Summary of the U.S. presidential election process. U.S. Embassy & Consulate in Thailand. Retrieved 8 February 2022, from https://th.usembassy.gov/summary-of-the-u-s-presidential-election-process/.

Syria's Assad wins 4th term with 95% of vote, in election the West calls fraudulent. Reuters. (2021). Retrieved 2 November 2021, from https://www.reuters.com/world/middle-east/syrias-president-bashar-al-assad-wins-fourth-term-office-with-951-votes-live-2021-05-27/.

Tambouris, E., Whimmer, M. A., Scherer, S., & Appel, M. (2015). *Electronic government and electronic participation: Joint Proceedings of ongoing research, Phd papers, posters and workshops of Ifip Egov and ePart 2015*. IOS Press.

Taş, R., & Tanrıöver, Ö. (2021). A manipulation prevention model for blockchain-based e-Voting systems. *Security And Communication Networks*, *2021*, 1-16. doi: 10.1155/2021/6673691.

State Duma. (2020). *The draft bill on the federal law on the amendments to the parts one and two to the code of tax of the Russian Federation, No. 1065710-7*. Moscow. Retrieved from https://sozd.duma.gov.ru/bill/1065710-7.

The National Academies Press. (2018). Ensuring the Integrity of Elections. In *Securing the vote: Protecting American democracy* (pp. 85-94). Retrieved from https://doi.org/10.17226/25120.

Thielman, S. (2015, April 15). *Voting machine password hacks as easy as 'abcde', details Virginia State Report*. The Guardian. Retrieved March 22, 2022, from https://www.theguardian.com/us-news/2015/apr/15/virginia-hacking-voting-machines-security.

Top 5 Countries with the Most Skilled Workers in 2021. Global PEO Services. (2022). Retrieved 24 February 2022, from https://globalpeoservices.com/top-5-countries-with-the-most-skilled-workers-in-2021/.

Tusk Strategies. (2021, November 1). Retrieved March 21, 2022, from https://tuskstrategies.com/team-member/bradley-tusk/Â

Tsahkna, A. (2013). E-voting: lessons from Estonia. *European View*, *12*(1), 59-66. https://doi.org/10.1007/s12290-013-0261-7.

United States Election Assistance Commission (EAC). (2015). *EVM testing & certification program manual, version 2.0* [Ebook] (pp. 1-79). Silver Spring, MD. Retrieved from https://www.eac.gov/sites/default/files/eac_assets/1/28/Cert%20Manual%207%208%2015%20FINAL.pdf.

United States Agency for International Development (USAID). (2013). *Best practices in electoral security: a guide for democracy, human rights, and governance programming* [Ebook] (pp. 9-11, 22-28). Washington D.C. Retrieved from https://www.usaid.gov/sites/default/files/documents/1866/Electoral_Security_Best_Practices_USAID.pdf

Updike, J. (1995). Introduction. In J. Updike (Ed.), *Rabbit Angstrom: A tetralogy*. New York, London and Toronto: Alfred A. Knopf, Everyman's Library.

uPort Developer - Helping you build user centric apps on blockchains. Developer.uport.me. (2022). Retrieved 27 February 2022, from https://developer.uport.me/flows/tx.

US presidential election: how the votes are counted. The Straits Times. (2020). Retrieved 15 May 2021, from https://www.straitstimes.com/world/united-states/us-presidential-election-how-are-the-votes-counted.

Vermaas, P., Kroes, P., van de Poel, I., Franssen, M., & Houkes, W. (2011). *A Philosophy of technology: from technical artefacts to sociotechnical systems*. San Rafael, CA: Morgan & Claypool Publishers.

Videos show Trump protesters chanting 'count those votes' and 'stop the count' outside separate ballot-counting sites in Arizona and Michigan. Business Insider. (2021). Retrieved 15 May 2021, from https://www.businessinsider.com/videos-trump-protesters-michigan-arizona-vote-count-2020-11.

Virginia Information Technologies Agency (VITA). (2015). *Security assessment of WinVote voting equipment for department of elections - Commonwealth Security and Risk Management Report* [Ebook] (pp. 1-6). Retrieved 2 February 2022, from https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf.

Voatz, Inc. (2022). *A brief technical analysis of claims made by some researchers from MIT* [Ebook] (pp. 1-16). Retrieved 15 March 2022, from https://voatz.com/wp-content/uploads/2020/07/V-Analysis-of-MITresearchers-claims.pdf.

Voatz response to researchers' flawed report - Voatz. Voatz. (2020). Retrieved 15 March 2022, from https://voatz.com/2020/02/13/voatz-response-to-researchers-flawed-report/.

Vote counting at polling stations. Aceproject.org. (2021). Retrieved 15 May 2021, from https://aceproject.org/main/english/vc/vcb.htm.

Voter fraud map: election fraud database | The Heritage Foundation. The Heritage Foundation. (2021). Retrieved 2 November 2021, from https://www.heritage.org/voterfraud.

Voting methods and equipment by state - Ballotpedia. Ballotpedia. (2021). Retrieved 15 May 2021, from https://ballotpedia.org/Voting_methods_and_equipment_by_state.

Weiss, M., & Haylard, M. (2019). *Voatz*. Voatz - Case - Faculty & Research - Harvard Business School. Retrieved March 21, 2022, from https://www.hbs.edu/faculty/Pages/item.aspx?num=56024

Weinstein, L. (2019). *University of Michigan students implicated in potential voting app hack*. The Michigan Daily. Retrieved March 20, 2022, from https://www.michigandaily.com/news/news-briefs/university-michigan-students-implicated-potential-voting-app-hack/

Werner, A. (2019).Â *WV secretary of State to deter threats against election systems and Processes*. Secretary of State Mac Warner. Retrieved March 19, 2022, from https://sos.wv.gov/news/Pages/10-2-2019-A.aspxÂ

Wegryzn, K., & Wang, E. (2021). *Types of blockchain: public, private, or something in between: Foley & Lardner LLP*. Blogs | Manufacturing Industry Advisor | Foley & Lardner LLP. Retrieved March 18, 2022, from https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

What is a blockchain fork?| CMC Markets. Cmcmarkets.com. (2022). Retrieved 7 March 2022, from https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-a-blockchain-fork.

What is digital identity?. Avast Security News Team. (2022). Retrieved 11 March 2022, from https://blog.avast.com/what-is-digital-identity-avast.

What is hyperledger fabric? | IBM. Ibm.com. (2022). Retrieved 9 February 2022, from https://www.ibm.com/topics/hyperledger.

What are smart contracts on Blockchain? IBM. (n.d.). Retrieved March 18, 2022, from https://www.ibm.com/topics/smart-contracts

White, J., Sutton, S., Sitrin, C., Mahoney, B., & Gerstein, J. (2022). *How to hack an election in 7 minutes*. POLITICO Magazine. Retrieved 17 March 2022, from https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144/.

Whitepapers - Voatz. (2022). Retrieved 15 April 2022, from https://new.voatz.com/whitepapers/.

Zawicki, K. (2018). *Keyless signature infrastructure (KSI): blockchain technology for the defense industry* [Ebook]. Guardtime Federal. Retrieved 14 February 2022, from https://potomacinstitute.org/images/VITAL/2018-08-16-KSI---Blockchain-Tech-for-DoD.pdf.

Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A., & Huang, S. (2018). A privacy-preserving voting protocol on blockchain. *2018 IEEE 11Th International Conference On Cloud Computing (CLOUD)*. doi: 10.1109/cloud.2018.00057.