Agora

Bringing our voting systems
into the 21st century

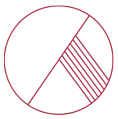
Whitepaper
Version 0.2

DISCLAIMER

The attached whitepaper is meant to describe the currently anticipated plans of Agora and its affiliates (together, "Agora") for developing a new blockchain token mechanism ("Token") that will be used on the network sponsored by Agora ("Network"). Nothing in this document should be treated or read as a guarantee or promise of how Agora's business, the Network, or the Tokens will develop or of the utility or value of the Network or the Tokens. This whitepaper outlines Agora's current plans, which could change at its discretion, and the success of which will depend on many factors outside Agora's control, including market-based factors and factors within the voting and cryptocurrency industries, among others. Any statements about future events are based solely on Agora's analysis of the issues described in this document. That analysis may prove to be incorrect.

This document does not constitute an offer or sale of the Tokens or any other mechanism for purchasing the Tokens (such as, without limitation, a fund holding the Tokens or a simple agreement for future tokens related to the Tokens). Any offer or sale of the Tokens or any related instrument will occur only based on definitive offering documents for the Tokens or the applicable instrument.

Purchasing the Tokens or any related instrument is subject to many potential risks. Some of these risks will be described in the offering documents. These documents, along with additional information about Agora and the Network, are available on our website at https://agora.vote/. Purchasers of Tokens and related instruments could lose all or some of the value of the funds used for their purchases.



1. AGORA

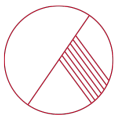
Formed in 2015, Agora is a Swiss-based voting technology company that has developed an end-to-end verifiable voting solution for governments and institutions. Today's voting systems are slow, costly and exposed to many vulnerabilities that can inhibit free and fair elections. Our team of skilled cryptographers and security scientists has built a blockchain-based solution to provide our partners with a modern, provably secure and cost-effective manner of engaging voters. Elections on Agora's network are tamper-proof throughout the entire voting process and offer full transparency to voters, third-party auditors and the general public.

Our team is passionate about spreading fair and transparent elections around the world, and we believe Agora has the potential to offer great value for global human rights. Agora was born from the combined work of Bryan Ford, who served as the Director of the Swiss Federal Institute of Technology Lausanne's (EPFL) Decentralized and Distributed System Lab (DEDIS) alongside his team of engineers and researchers, and Leonardo Gammar, an accomplished entrepreneur passionate about blockchain, who grew up in diplomatic circles.

Our team of cryptographers has already implemented several large-scale blockchain projects and has many years of experience in providing digital solutions for electoral systems. Of particular relevance, our team previously developed several centralized e-voting frameworks for Swiss Post and the State of Geneva before beginning work on Agora.

Agora stands out as the first blockchain voting solution that is architected to meet the performance needs of a mission critical election. Our technology runs on a custom blockchain that our team has been developing since 2015. In this whitepaper, we present three technological innovations developed by our team: Skipchain, Cotena and Valeda. Skipchain provides a consensus mechanism with high throughput and efficient transaction validation. Cotena then provides a method for storing cryptographic Skipchain proofs onto the Bitcoin blockchain. Finally, Valeda performs cryptographic proofs validating Skipchain and Cotena data. Our architecture provides end-to-end verifiability with a high level of security.

At the core, our company and technology strive to meet the evolving needs of modern voters. Not only do voters demand greater transparency in their elections, but they also demand more convenient methods of participating. Over the long run, we seek to enable any authorized voter to participate in an election through their own digital device, all while guaranteeing the security and transparency of the electoral procedure.



To understand how Agora's approach to blockchain voting succeeds where traditional systems have struggled, we have developed a template of characteristics that are necessary for election results to be trusted. A free and fair election must minimally satisfy the following requirements:

TRANSPARENCY

Each step of the election process should be easily understood and open to scrutiny by all stakeholders (voters, political parties, outside observers and others). All results should be independently verifiable and auditable.

PRIVACY

The choices that each voter makes should remain private both during and after the election.

INTEGRITY

Only eligible voters should be allowed to vote, and those votes must be protected from any alteration or exclusion.

AFFORDABILITY

The election process must be affordable to governments and its citizens in order to maintain sovereignty.

ACCESSIBILITY

All eligible voters, regardless of location, group membership or disability, should have reasonable and equal opportunity to cast their ballot.

1.1. MISSION

Agora endeavors to spread fair and transparent elections around the world with end-to-end verifiable blockchain voting technology. To realize this mission, we have spent the past two-and-a-half years assembling, what is in our view, a highly capable team and technology that can meet the evolving needs of voting administrators. Agora's voting solution satisfies all of the requirements that we believe are necessary to ensure a free and fair election, including transparency, privacy, integrity, affordability and accessibility.

Blockchain is the key technology that unlocks this mission. Blockchain provides a trustless, digital and decentralized method of generating cryptographically secure records, which also preserve the anonymity of participants while remaining open to public inspection. Applied to voting, blockchain ensures that votes are recorded accurately, transparently, permanently and securely.

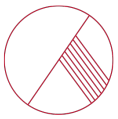
1.1.1. TRANSPARENCY

Agora's voting solution offers full transparency and public verifiability over the entire voting process, including to third party observers. This is achieved through Agora's public blockchain, called the *Bulletin Board*, where data is stored throughout the election process. Any party can verify the validity of an election as well as all intermediate steps of the voting process.

In addition to permitting outside analysis, Agora enables each voter to verify that his or her vote was accurately recorded and that it remained unaltered. In this way voters play a key role in ensuring a fair election and can place their trust in the electoral procedures. Election results are also publicly available to all stakeholders on our blockchain along with cryptographic proofs of their validity.

1.1.2. PRIVACY

Agora's platform protects voter privacy through verifiable ballot encryption and anonymization. The cryptographic methods that we use to ensure privacy come from widely researched and accepted models, including threshold ElGamal for ballot encryption and Neff shuffling for ballot anonymization.



Equally as important, Agora does not have access to user data, including the content of voter ballots. All ballots are encrypted on each individual's voting device using open source encryption algorithms before being transmitted to Agora's network. Once ballots are on our network, they are anonymized to detach votes that will be tallied from the credentials of any given voter.

1.1.3. INTEGRITY

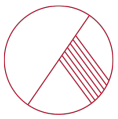
The central strength of any blockchain solution is cryptographic security. Maintaining the integrity of the elections that occur on our network is of the utmost importance to our company, and our technology has been built to transparently ensure this. Ballots and final election results cannot be altered by any third party, including Agora, at any point throughout the voting process. Blockchain is the key component of our architecture that protects against intervention from governments, institutions, third parties and others who may seek to subvert the election process.

Agora's blockchain, which is maintained by a distributed network of independent witness servers called the Cothority, requires consensus from a defined threshold of Consensus Nodes and keeps a verifiable record of all voting data, including encrypted individual ballots and proofs to verify that data from each step of the voting process remains unaltered. Our blockchain provides public, cryptographic proof that results have not been manipulated in any way.

1.1.4. AFFORDABILITY

The efficiencies generated through a blockchain voting system can be radical. Cost reductions begin from the digitization of paper and manual processes, and they can be further driven through the cryptographic auditing capabilities that a well-architected blockchain platform provides. When digital means of voting are used in a way that does not require substantial manual auditing, election costs go down while producing enhanced reliability in the results. In the long run, when digital voting can be achieved from an individual's own home, the costs associated with maintaining and securing physical polling stations will largely disappear as well.

The operational and security costs of administering an election can be staggering. For jurisdictions with limited economic means and strong political tensions, the issue of financing elections can have a wide impact, even limiting a nation's sovereignty. Agora seeks to provide a path to such states so they may avoid going into debt in order to organize elections, which would otherwise increase their dependence on external influences. We believe that Agora's technology



can reduce some nations' dependence on foreign aid as well as the risk of outside interference in their internal affairs, thereby strengthening their sovereignty.

1.1.5. ACCESSIBILITY

Agora's solution can enable secure and remote voting from digital devices, including personal computers and mobile phones. Our ultimate goal is for voters to be able to vote from anywhere using our technology, removing the need to physically travel to polling stations in order to participate in an election. A mobile solution such as this better fits the lifestyle of modern voters, who are presently required to use outdated voting techniques.

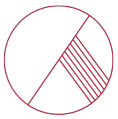
The importance of accessibility goes beyond simple convenience and creates new ways of ensuring election fairness. There have been numerous recorded incidents globally in which valid voters have been prevented from participating in an election because of the actions of an imposing force, such as a political party or armed faction. The ability to vote from a personal device outside of an election facility can mitigate the impact these groups may have on an election.

1.2. OUR CUSTOMERS

Agora provides governments and institutions with the resources they need to run credible elections, whether in-person or on their citizens' own devices. The solution is highly scalable, capable of running elections at any jurisdiction level from cities to sovereign nations. However, our technology is not confined solely to nations. Any organizations with wide-scale voting needs, such as public companies, will also benefit from holding their votes and elections on the platform.

1.2.1. PROVIDING VALUE

We believe that our platform adds meaningful value to governments over the existing voting platforms on the market today, which are not currently based on blockchain technology and do not possess comparable capabilities. These systems have been consistently shown to be vulnerable to hacks and outside manipulation, as was recently demonstrated at the DEF CON security conference, where a voting machine presently used in U.S. elections was hacked within 90 minutes.



1.2.2. REDUCING COSTS

Agora's technology has the potential to create new efficiencies that provide cost savings for governments. Based on our estimates, we believe that use of Agora may be able to provide election administration cost savings between 50% and 80% versus other options.

1.2.3. INTEGRATION

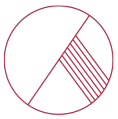
It can be challenging to implement complex voting technology that serves an entire nation's population. Furthermore, with a diverse array of laws, election rules and voting frameworks between governments, our customers have unique needs that must be met in order for Agora to be recognized as the right voting technology provider. Agora's team will therefore oversee all integrations and proper functioning of systems before and during elections to ensure that adopting our technology is successful.

Our custom solutions will be developed on top of Agora's core platform presented in this white-paper and will offer each voting administrator the ability to integrate our technology into its own electoral procedures.

1.2.4. GLOBAL VALUE

Political stability and fair elections directly impact the trust given to governments by the international community and investors. Foreign investors have consistently rewarded countries that support a rule of law, protection of human rights and policies that prevent high-level corruption. Earning trust from the international community and foreign investors is therefore a high priority for most nations.

Taking a lead on this societal push is our local partners. The official and unofficial partners who support Agora within their countries become public leaders for voting transparency and fairness. Advocates of Agora's verifiable voting technology demonstrate a commitment to a transparent election process that we believe every company should make. By supporting this global issue locally, our partners have an opportunity to stand out in their respective nations. Agora's team will work to establish a dialogue and supportive relationship with each of our partners by providing tangible evidence of their efforts to prevent corruption, which is a major factor in the disruption of healthy economic relations abroad.



Agora is not politically affiliated. We are a neutral organisation that will never interfere in elections in any way.

2. CONVENTIONAL VOTING SYSTEMS

The voting systems used in most countries today are inefficient and outdated. In most cases, citizens must still personally visit polling stations and complete a ballot using manual, error-prone processes. Many eligible voters ultimately decide to forego participation in elections due to the challenges and frustrations presented by antiquated voting systems.

Even when voters participate, there are often questions concerning the integrity of the election process that may cause the final outcome to be questioned. Without a cryptographically secure architecture that allows voters to confirm that their own vote has been accurately recorded, current voting systems fail to satisfy their primary objective of relaying people's voices accurately. The problems faced by traditional solutions are pervasive and well-documented, as outlined in the following sections.

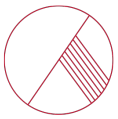
2.1. ELECTRONIC VOTING MACHINES

Around 31 countries worldwide have experimented with non-remote Electronic Voting Machines (EVMs) as a whole or part of their election system. Currently only 20 countries actively employ them. [1] Concerns about their security and transparency have led to these programs being discontinued throughout much of Europe, including France, Germany, the Netherlands and Ireland. These systems also present issues around affordability. While EVMs can mitigate some of the costs associated with paper ballots, such as human tabulation and ballot printing, they impose a host of new costs, including buying, updating, storing and servicing the machines.

2.1.1. EVM TRANSPARENCY ISSUES

Black Box Architecture

Direct Record Electronic (DRE) systems, particularly those without a Voter-Verified Paper Audit Trail (VVPAT), are intrinsically opaque since a vote is only recorded in the DRE computer's memory. Results produced by DRE systems without a VVPAT cannot be audited, since there is



no audit mechanism to compare against the machine's memory. Even with a VVPAT, the integrity of these black box systems is not guaranteed, as it is possible to compromise the software interfacing between the machine and the VVPAT, thereby altering both results. [2] Most voters fail to detect errors in VVPAT record after they have finished their ballot, which diminishes its ability to act as a failsafe against hacks and other vulnerabilities. [3]

No Open Source Code

Another transparency issue that beleaguers many EVMs is the proprietary nature of their source code. Without open source code, the election is effectively at the mercy of third-party providers. This is not just an issue of potential misconduct by these providers—errors in their code could result in changes in the election outcome that would be very difficult to detect.

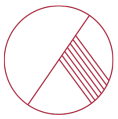
2.1.2. EVM INTEGRITY ISSUES

Security Vulnerabilities

DREs have been consistently shown to be vulnerable to a variety of cybersecurity attacks, including the insertion of malicious code which then propagates through links in the electronic voting system's network. [4] In the Netherlands, critics were able to expose these vulnerabilities, the existence of which were denied by the machine suppliers, by reprogramming one of the voting machines to play chess. [5] While machines that are connected to the internet or phone systems are the most vulnerable to security issues, these are not the only vectors through which hostile code could be inserted. If the DRE employs a voting card for identification, the cards can be altered to upload malicious code upon insertion. This form of attack, known as an "air-gap attack," has been successfully demonstrated by security researchers. [6] These are just a few of the many security vulnerabilities that have plagued EVMs.

Outsourcing Vulnerabilities

Another issue is that hangs over the use of EVMs is the challenge of their implementation. As official election staff may lack the proper training and IT skills needed to manage machines themselves, the machines' on-site servicing and management is often outsourced to the EVM supplier. [5] This effectively outsources the integrity of the election to the EVM supplier as well. The supplier's special knowledge allows it to act without effective supervision, and consequently, if even one or a few individuals are subverted, they could easily alter an election by inserting malicious code.



Central Tabulator Vulnerabilities

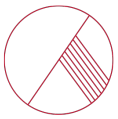
Systems that rely on centralized vote counting machines increase the ways in which an election's results can be subverted. Central tabulators have been shown to be vulnerable to attacks, just as voting machines themselves. For example, the GEMS central tabulator, which integrates with Diebold machines, can be effectively taken over by entering a 2-digit code in a hidden location. Anyone with physical access to the machine would then have complete control of election results. [7]

2.1.3. EVM COST ISSUES

Although EVMs avoid some of the associated printing costs of paper ballots, they are quite expensive in their own right. EVMs cost between US$3,000 to $5,000 each, and approximately one DRE machine is needed per 180 voters. [8] However, the upfront cost of purchasing machines is only a fraction of the total cost of operating these systems. The cost of programming voting machines can range between US$250 to $1,500 per machine every election. [8] Maintenance costs another US$100 to $250 per machine every election. [8] Software must also be re-licensed each year, and the machines must be stored in secure and air-conditioned locations. In sum, the cost of running an election with EVMs can be striking.

Machine Lifespan

Perhaps the highest cost associated with EVMs is machine lifespan. The estimated lifespan for most DRE systems is only about 10 to 20 years, after which time they must be replaced. [9] For the US, which was one of the early adopters of EVMs, a staggering US$1 Billion is presently required to replace its aging fleet of machines. It is critical that these machines be replaced as soon as possible. Not only do machine breakdown cause delays on election day, but older EVMs are far more likely to be subverted by hackers. For example, the U.S. state of Virginia's recently decommissioned WinVote machines were vulnerable to a security breach because the wireless cards that they employed used outdated Wi-Fi encryption standards. [9] Accuracy is another issue associated with older voting machines. The AccuVote TSX machine was shown to register incorrect votes when it aged due to a slippage of the touch screen as the glue holding it in place degraded. [9]



Polling Stations

Machines and equipment are only part of the cost associated with non-remote EVMs. Just as in paper ballot systems, polling stations must be established, outfitted, staffed and secured. In fact, these stations often incur greater costs than paper ballot systems.

2.2. PAPER BALLOTS

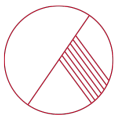
Most of the world currently uses some form of paper ballot as their primary voting system. Paper ballot systems have a number of advantages. Since paper ballots are relatively easy to mark secretly and track if the right protocols are in place, they generally satisfy requirements for both transparency and secrecy. They can, however, run afoul of a number of problems with regards to cost, integrity and accessibility.

2.2.1. PAPER BALLOT COST ISSUES

There are substantial expenses that make traditional paper ballots voting a costly endeavor for governments, and ultimately their citizens.

Paper and Materials

Sealing envelopes and transporting election materials alone accounted for 40% of the cost of the 2012 French presidential and legislative elections. [10] From ballot papers and information leaflets to electoral cards, each item must be printed and routed physically to voters or polling stations. These costs are further increased in the case of legislative elections, where there are more candidates requiring more materials to be produced. Colombia, for example, had to print 102 million ballot papers during its 2014 parliamentary elections, even though the country only had 32 million voters. [11] This reliance on costly materials discourages administrations from considering alternative electoral procedures, such as proportional voting, which would require even more printed materials and create additional costs. The structure of an entire electoral system can be determined strictly by financial constraints.



Polling Stations

Establishing a network of polling stations across an entire nation can be both complex and exorbitantly expensive. Voting administrators must first find suitable locations within the community, which must be purchased or leased if they are not public property. These stations must then be furnished with equipment, including voting booths, ballot boxes and other administrative machinery. Voting equipment itself can be quite pricey too. For example, the optical analysis machine deployed at each central counting office in the United States runs between US$70,000 and $100,000. [12]

Labor

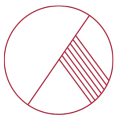
From personnel manning polling stations to those in charge of mailing and registering voters, election administrators must hire and train many employees to assist them. The labor costs associated with administering an election are high and not reduced by economies of scale. In the 2017 UK general election, £22 million (15%) of the £140 million election budget was spent on employee engagement and training. [13]

Voting administrators must also ensure the protection of voters, particularly those who are exposed to potential security threats triggered by extreme partisanship. In Kenya, where the incidence of election-related violence is high, approximately 600 people were reportedly killed following disputes over the results of its 2007 presidential elections. [14] In 2017, election-related violence remained the primary source of concern for a majority of Kenyans. [15] This issue also translated into substantial costs for the Kenyan government, who were forced to dedicate upwards of US$53 million for security alone in its 2017 general election.

2.2.2. PAPER BALLOT INTEGRITY ISSUES

Corruption Vulnerabilities

For any election system that is centrally governed, the integrity of the system depends directly on the trustworthiness of its administrators, who often have a vested interest in the election results. Multi-party democratic elections have become standard globally, but up to sixty regimes can be classified as “electoral authoritarians”—places where elections are held to stave off international and domestic criticism but whose results are manipulated by the ruling faction. [16]



Vulnerabilities exist throughout the voting process from start to end. The quantity, location and security of polling stations provide a ready handle to manipulate results, which can be used as a deterrent for voters who wish to avoid all-day lines or risks to their physical safety. Paper ballots can be directly manipulated too. In Nigeria's 2003 election, ballot boxes were stuffed in full view of independent observers. [16] In Egypt's 2005 presidential election, entire ballot boxes were discarded enroute to the counting facility. [16] Even if all of the ballots counted were produced by legitimate voters, methods further down the election process can alter outcomes too. Since tabulators have discretion over which votes to validate or invalidate when a ballot has an irregularity, corrupt officials can skew results by only invalidating only the ballots of the opposition.

Human Error Vulnerabilities

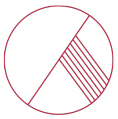
Fraud and corruption are not the only way in which paper ballots can stumble; they are also vulnerable to human error. Ballots can be lost or misrecorded by accident. Physical errors on a ballot may force tabulators to guess the intentions of the voter or discard the vote altogether. Physical counting processes, which can be completed by machine or by hand, are often inaccurate. In an experimental audit, researchers revealed that different groups of auditors reach different tallies close to 40% of the time, and that the average error percentage for any given candidates count was 1.4%, enough to swing any close election. [17]

2.2.3. PAPER BALLOT ACCESSIBILITY ISSUES

Impact of Locations

Paper ballots demand the selection of polling locations throughout a country in order to guarantee privacy and integrity. Depending on how many stations are established and where, travel can be a barrier to voter participation. Some rural voters live hours away from their nearest polling station, and even in major cities, visiting a station often takes substantial time. Furthermore, minor changes in the location of polling stations can have a meaningful impact on overall turnout and can be used to sway who decides to participate in an election.

Travelling to the polling site is only half the battle. Once the voter arrives, waiting times can also be high enough to discourage voters. In a recent US election, some voters experienced a wait time of six to seven hours. [18]



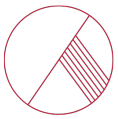
Voters with Disabilities

Some segments of the population are particularly vulnerable to being excluded from current electoral system. Voters with disabilities, such as those with impaired vision, are the most affected by systems that require them to physically travel to polling stations. These stations are often not equipped to receive them and can fail to provide ballots that cater to their needs. While alternatives such as voting by mail or proxy voting exist in some countries, they are not a widespread option globally.

2.2.4. PAPER BALLOT INEFFICIENCY ISSUES

It can take substantial time and resources to administer an election using current voting systems. These efficiencies are largely due to logistical issues in deploying physical election resources, excessively long tally processes and more. The 2014 India parliamentary elections are one of the most striking recent examples of the difficulties inherent in deploying a network of physical polling stations. Due to the country's immense geographical size, its elections were divided into nine rounds spread out over an entire month, as security forces needed time to move from one area of the country to another.

The tallying of ballots can also generate inefficiencies and long delays. Constrained by unwieldy counting procedures and a slow manual recount, the final results of Ukraine's 2014 parliamentary election were not available until 15 days after the election took place. [19]

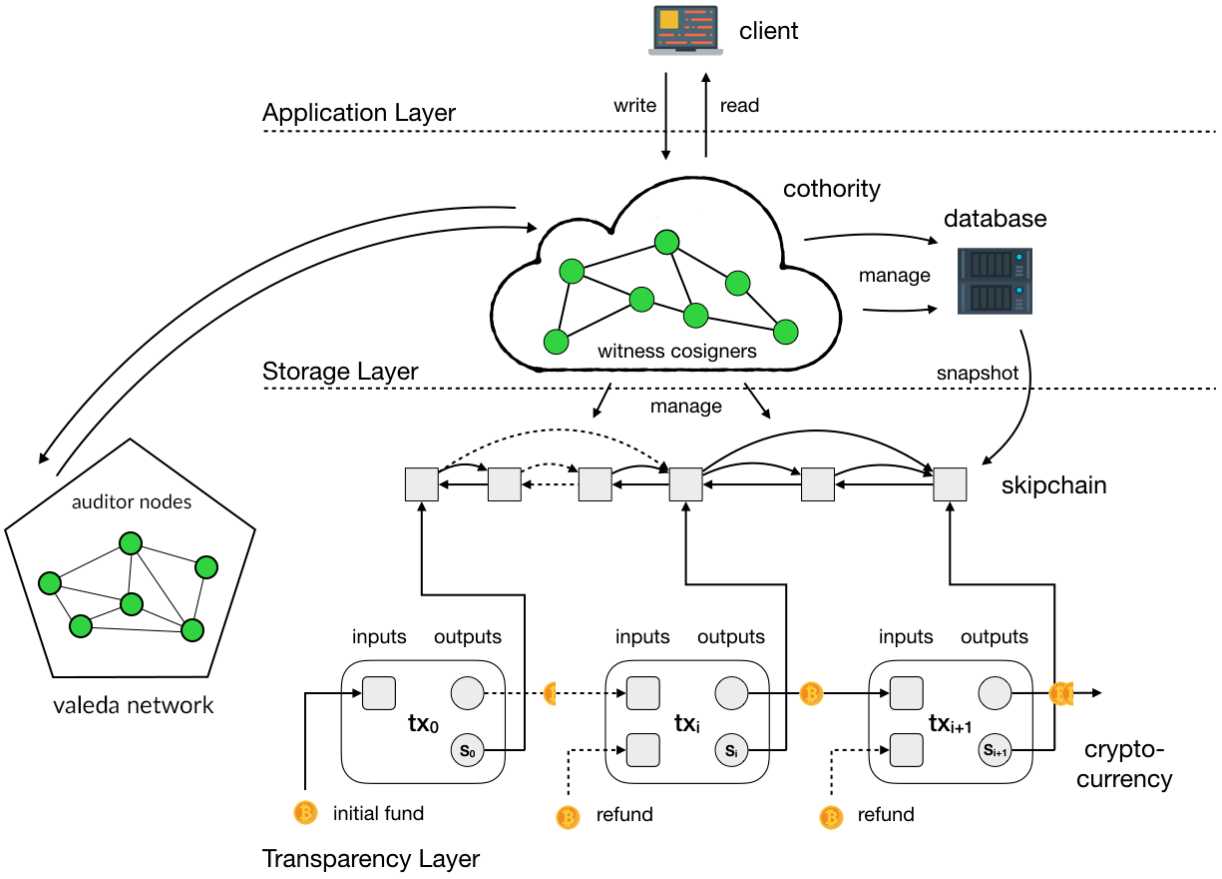


3. TECHNOLOGY

Agora has built a multi-layer architecture that is based on blockchain technology, which includes several innovations that have been developed by our team. Agora's blockchain, called the *Bulletin Board*, is a distributed permission ledger based on the Skipchain architecture, which we have been developing since 2015. Data on our *Bulletin Board* is cryptographically tied to the Bitcoin blockchain through our *Cotena* layer, which provides a high level of immutability and decentralization of our data. The system we have architected provides high throughput capabilities and low overhead, which enables Agora to be run on low bandwidth devices.

3.1. LAYERS

Agora is composed of five technology layers: the *Bulletin Board* blockchain, *Cotena*, the Bitcoin blockchain, the *Valeda* network and *Votapp*. These layers communicate with each other at various instances throughout the election process to provide a cryptographically secure voting environment with auditable proofs. A visualization of our technology layers is provided below.



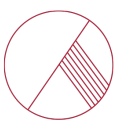
3.1.1. BULLETIN BOARD BLOCKCHAIN

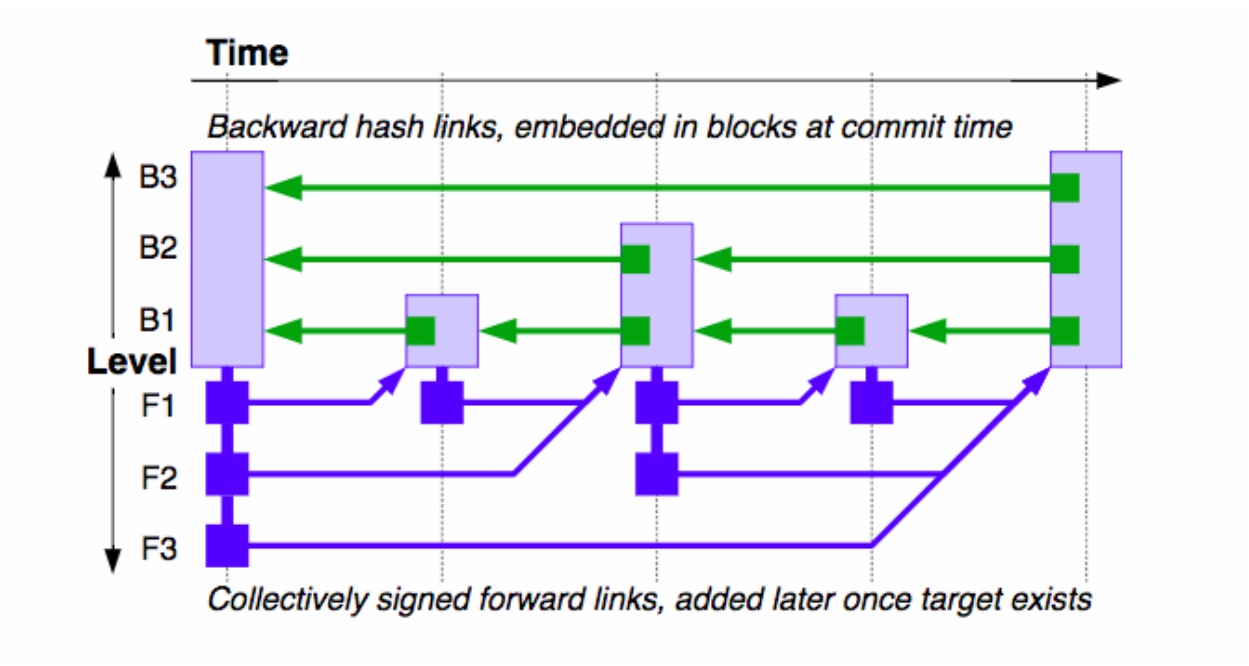
The Bulletin Board is the permissioned blockchain of the Agora network, which consists of write-permissioned nodes operated by Agora and recognized third-party witnesses (Consensus Nodes) as well as read-only nodes (Citizen Auditor Nodes) that can be operated by anyone in the world. This blockchain network provides an immutable record of all data throughout the election process and acts as the central communication channel, memory and permanent data store of our system. The Bulletin Board is a distributed append-only database to which any party, given the right authentication, can post signed messages and statements. This process of sending cryptographically signed and authenticated data to the blockchain keeps the entire election process on Agora's platform secure, private and auditable.

Skipchain Architecture

The Bulletin Board layer is based on Skipchain [52] architecture, which provides a proactive Byzantine consensus mechanism with high throughput and efficient transaction validation. The Skipchain data structure was first introduced by our team at Usenix Security 2017 in our Chainiac paper. [52]

Skipchains enable software clients to efficiently navigate arbitrarily long blockchain timelines both forward and backward, providing proof of transaction validity without the need for a full record of the blockchain. Back-pointers in Skipchains are cryptographic hashes, while forward-pointers are collective signatures by a group of witnesses. Skipchains are a useful cryptographic blockchain structure loosely inspired by skip lists. [20] The fundamental concept of a skip list is to augment a conventional singly-linked or doubly-linked list with additional long-distance links, which are structurally redundant but allow much more efficient traversal and search across arbitrary distances along the timeline in a logarithmic, rather than linear, number of steps. We adapted the skip list idea to blockchains by adding long-distance links both forward and backward in time, as illustrated below.

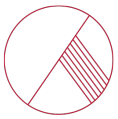




In this way, our software can validate a referenced block by using cryptographically validated markers that represent a large group of adjacent blocks. The end result is that even resource-constrained clients, such as those on mobile phones, can obtain and efficiently validate binary updates using a hard-coded initial software version as a trust anchor. Such clients do not need to continuously track a release chain, like a Bitcoin full-node does, but can privately exchange data and independently validate blocks on-demand due to the Skipchains forward and backward links being offline verifiable.

Each block in the Skipchain consists of the following data elements:

- Root hash of the Merkle tree containing all transactions in the current block;
- Root hash of the Merkle tree representing the entire Skipchain's current state;
- Hash of the current block, which acts as a unique identifier for the current block;
- Hash backward link pointing to the previous block;
- List of forward and backward links pointing to different blocks in the Skipchain for quick navigation within the chain;
- List of Cothority nodes responsible for handling that block.



Cothority

The nodes that secure the Bulletin Board consist of a permissioned collective authority ("Cothority") that confirms transactions. As is standard with other blockchains, each node in the network maintains a copy of all transactions and approves new transactions into blocks as part of the network's consensus mechanism. Nodes independently monitor each other to ensure that the system's data record remains unaltered.

The Cothority on our platform consists of a set of Consensus Nodes that collectively confirm transactions onto the Bulletin Board. Transactions can consist of various data elements used on Agora, including ballots, the configuration file and consensus proof. From the set of Consensus Nodes, one of the nodes is designated to be an 'oracle node' on a rotating basis. The rotating oracle node receives ballots and other data from the Consensus Nodes, proposes new blocks to the network and writes confirmed blocks to the Cotena log, which is discussed later. The oracle and Consensus Nodes on Agora's network are operated in distinct physical locations by Agora and independent third parties.

Consensus Nodes in the Cothority serve the following purposes:

1. Maintain a copy of our blockchain, the Bulletin Board.

2. Receive encrypted ballots from voters and authenticate their data, ensuring that ballots were sent by an authorized voter.

3. Confirm blocks proposed by the oracle server.

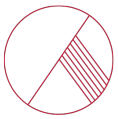
4. Decrypt anonymized ballots once the election has ended, creating plaintext ballots that can be tallied.

5. Maintain a copy of the Cotena log and monitor its correctness.

The oracle server, which is selected randomly from one of the Consensus Nodes on a rotating basis, serves the following purposes:

1. The oracle adds the configuration file to the Bulletin Board.

2. The oracle creates blocks from authenticated ballots received by Consensus Nodes and proposes them to the network for confirmation.



3. The oracle adds confirmed blocks to the log and pushes them to the Bitcoin blockchain.

The Bulletin Board architecture offers a scalable blockchain infrastructure that that can handle the specific data needs of elections administered on Agora.

3.1.2. COTENA

The permissioned Bulletin Board interacts with our second layer, Cotena, which is based on the Catena schema [58]. Catena is a tamper-resistant logging mechanism built on top of the Bitcoin blockchain. This layer links the Bulletin Board and supporting cryptographic proofs to the Bitcoin blockchain, which provides decentralized immutability to our permissioned layer's data.

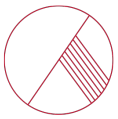
In the Cotena layer, the Cothority manages an append-only log that is formed from a chain of select Bitcoin transactions, where application-specific statements are made via the OP_RETURN opcode. Because of this design, clients running Agora software need only to download Bitcoin block headers and small Merkle proofs under some of those headers. After all block headers are downloaded, the network bandwidth required decreases to less than 1 KB of data every 10 minutes. Since modifying data in the Cotena log would require one to double-spend on the Bitcoin blockchain, the schema achieves the immutability of Bitcoin without its overhead.

The high costs and data inefficiencies of the Bitcoin blockchain, which has surpassed 150 GB in size, make it no longer practical for full nodes to operate on every device. Cotena was created to leverage the data security of the Bitcoin blockchain while introducing a design that has minimal data storage requirements and reduced Bitcoin transaction costs.

Cotena Log

The Cotena log is a list of Bulletin Board snapshots taken periodically over time. A copy of each log update is saved both by the Cothority nodes and on the Bitcoin blockchain.

To create a Cotena log, the Cothority generates a new collective Bitcoin address, then signs and broadcasts a Cotena 'genesis' transaction tx0 to the Bitcoin network. This transaction includes the Cothority's public key as the statement s0 and pays an initial amount of bitcoin b0 to the newly generated address. To extend the log, the Cothority broadcasts a Bitcoin transaction txi with a statement si such that txi credits an amount of bitcoin bi-1 from the output of txi-1 back to the Cothority's address, less transaction fees. This procedure produces a transaction chain



that builds a tamper-resistant log of statements s0 , s1, ..., si that is as difficult-to-fork as the Bitcoin blockchain itself.

The Cotena log can be extended until it runs out of funds. To add more funds to the log, Cotena transactions can have additional inputs that lock extra funds into that transaction's continuation output. These inputs can only be used to add extra funds and cannot be used to maliciously join two different logs, since Cotena only uses their first input to spend previous Cotena transactions. Nodes running Agora clients can easily detect if a Cotena transaction tries to point to two distinct previous Cotena transactions from the additional inputs.

A predefined threshold (e.g. two-thirds) of Consensus Nodes in the Cothority must approve any extension of the log that is to be made. For a statement to be sent to Cotena, it must be approved in a signed transaction by the Cothority. In this process, Consensus Nodes can ensure that each transaction txi fulfils certain conditions before it is added to the Bitcoin blockchain.

This includes checks such as:

- The transaction txi has the correct data format to prevent a compromised member of the Cothority from ending the log with a malformed transaction.

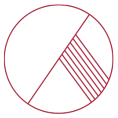
- The statement si included in txi is compliant with the application and does not corrupt the application state.

- The transaction txi uses the first input to spend the output of txi-1 to avoid a malicious merge of two distinct logs.

- The transaction txi credits the log's address and not a different address controlled by an attacker or malicious authority that wishes to censor client messages.

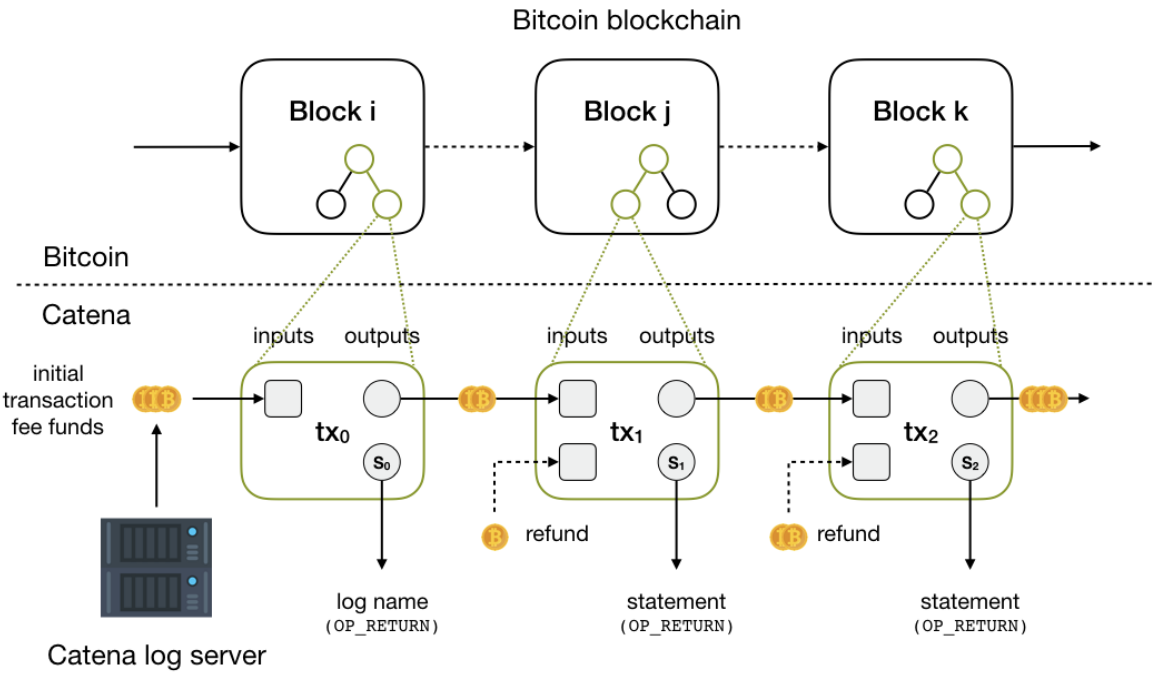
At the initialization of this second layer, Cotena includes not only details about its collective public key in the genesis transaction tx0 but also a hash of the Bulletin Board's first Skipblock. Using that information, a client can verify that its Cotena log is recording Skipblocks from the correct Skipchain.

Once a Cotena log is initiated through a genesis transaction, its maximum log update frequency is bound to the block time of the underlying cryptocurrency. When deployed on top of Bitcoin, as is the case with Agora, Cotena can at most issue one log update every ~10 minutes. To solve this, transactions are recorded first to the Bulletin Board, and then a snapshot of its latest Skipblock is sent to Cotena by the current oracle node. The interval over which the Bulletin Board sends data to Cotena is called an epoch.



During an election, every ballot and other updates are recorded to the *Bulletin Board*, which can happen very frequently (e.g., once a minute). In less frequent intervals (e.g., once a day) the Cothority updates the Cotena transaction log with a hash of the latest Skipblock from the most recent epoch. This log update is then pushed to the Bitcoin blockchain for decentralized immutability and transparency. This approach enables Agora to scalably add ballots to a decentralized blockchain while attaining low costs and latency.

COTENA TRANSACTIONS



Bitcoin / Catena transactions

In order for interested parties to verify that the log updates on the Bitcoin blockchain are correct representations of the *Bulletin Board* and vice versa, cryptographic proofs provide a definitive validation that data remains correct.

Together, the *Bulletin Board* and Cotena provide a permissioned-and-permissionless hybrid blockchain configuration that achieve tamper-proof decentralization with low cost and high data throughput (qualities not associated with Bitcoin as a standalone blockchain).

They are the foundation of our system with no single points of failure, a configurable update frequency and offline verifiability.

3.1.3. BITCOIN BLOCKCHAIN

The Bitcoin blockchain is a digital, decentralized ledger that keeps a record of all transactions that take place across Bitcoin's peer-to-peer network. One major innovation of this technology is that it allows participants to store and transfer data across the Internet without the need for a centralized third party. Data stored on a decentralized blockchain is immutable to changes, making the blockchain a trustworthy source of data. The Bitcoin network is maintained by a decentralized network of miners who are rewarded in bitcoin, the most widely known cryptocurrency.

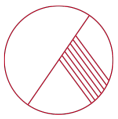
Agora uses the Bitcoin blockchain as a part of its broader architecture to store certain data that our system requires to be fully decentralized. The Bitcoin network is currently one of the the largest decentralized networks of computers in the world, and its blockchain is consequently considered to be highly secure and offer high immutability of data. Cotena periodically stores a hash of the most recent Skipblock in a Bitcoin transaction OP_RETURN opcode, which enables anyone to verify that the Cotena log and *Bulletin Board* remain unaltered.

3.1.4. VALEDA NETWORK

The Valeda layer of Agora is a global decentralized network of trustless nodes that validate election results on the Bulletin Board. This layer serves to provide final public evidence that the Cothority has maintained the authenticity of Bulletin Board data and that election results are valid. The Valeda network consists of Citizen Auditor Nodes whose software computes cryptographic proofs pertaining to various processes of our platform including ballot recording, anonymization, decryption, tallying and more.

Once an election period has ended and ballots have been computed by the Cothority, all Citizen Auditor Nodes in the Valeda network will run validations on the results.

Citizen Auditor Nodes are run by staking tokenholders who choose to enter a dedicated contract with Agora and conduct KYC. Under the terms of the contract they stake their tokens and audit remotely the elections at the end of which they receive payment tokens for the services they have rendered. The function of Citizen Auditor Nodes is explained in our Tokenomics section.



3.1.5. VOTAPP

Votapp is the application layer of the Agora network. Anyone can write applications on top of Agora to make interactions with the Bulletin Board user-friendly. Primary applications that will exist in the Votapp layer include Voting Booth, Audit and Node.

Voting Booth

The Voting Booth application allows authorized voters to participate in an election on Agora's network. This application downloads information from the election event's configuration file and displays relevant information, such as candidates and choices, to the voter. The voter is then able to select candidates and choices within their ballot, which is encrypted before being sent to the *Bulletin Board*. Finally, the Voting Booth application allows voters to ensure that the encryption mechanism on their device is working properly as well as confirm that their casted ballot has been added to the total tally.

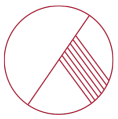
Audit

End-to-end verifiability is a core feature of Agora's voting technology, and the Audit application provides an accessible toolset for auditing an election at all points throughout the election process. Auditing can also be performed on each layer of Agora's architecture as well.

While we will provide a toolset to facilitate auditing through Valeda, anyone can audit Agora's technology or an election using their own custom code.

Node

Anyone can run a full Node on Agora's network, which maintains a full history of our Bulletin Board and Cotena logs. A full node can reply to any client's request to query the Bulletin Board but is not able to actively participate in the network by acting as a Consensus Node. In order for a node to operate as a Consensus Node, it must be evaluated as a partner of Agora to be authenticated on the network.



4. VOTING

Elections on Agora's network are administered through a methodical yet customizable voting process. The process we have designed for use in our system ensures that several technological requirements important to maintaining a valid election are fulfilled, including end-to-end verifiability, privacy, decentralization and scalability. Agora's technology is built to support these requirements, which enable governments and organization to hold elections on a fully-verifiable digital voting platform.

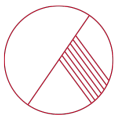
In this section, we discuss how elections work on Agora's platform throughout the various stages of the voting process. While this section is intended to be a non-technical overview, we will also reference how the actions carried out in each stage interact with Agora's various technology layers.

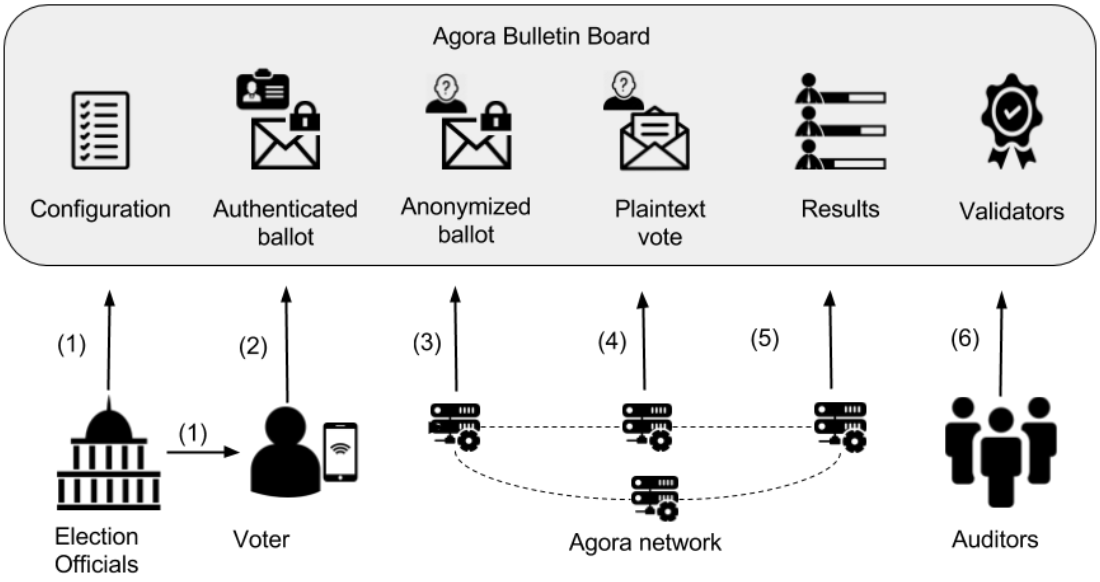
4.1. VOTING PROCESS

Agora's voting process consists of six distinct steps, which together provide for a cryptographically verifiable voting solution that merits the confidence of voters and the wider public. Elections on Agora's platform proceed according the following steps:

1. *Configuration:* Election administrators create a new election event.
2. *Casting:* Voters cast their encrypted ballots to Agora's network.
3. *Anonymization:* Agora's network anonymizes all voter ballots.
4. *Decryption:* Agora's network decrypts the anonymized ballots.
5. *Tallying:* All votes are counted.
6. *Auditing:* Auditors and observers post reviews confirming validity of election results.

A high-level overview of the voting process is pictured below, which displays how each step of the voting process is related to different participants within our ecosystem.





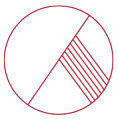
STEP 1: CONFIGURATION

Prior to administering an election, the administrators begin an election event by creating a configuration file, which includes event-specific parameters, such as the identities of the responsible officials, the eligible voters, the anonymization nodes, the start and end times of the casting phase, the election type, the list of available candidates and more. The full set of parameters include:

• *List of Election Officials.* These values include the names and public keys (identifiers) of the election officials. To increase resilience against failures, decentralize trust and keep the overhead of signing and verifying statements minimal, a single shared public key generated through a distributed key generation (DKG) protocol can be used.

• *Election Type*. This value determines the concrete voting mechanism, such as majority voting or single transferable voting (STV), and its parameters, e.g., how many options a voter can select in an STV.

• *Election Start/End Times.* These values specify the time frame in which eligible voters are allowed to cast their ballots. The compliance with this time frame is enforced by the Agora nodes as accurately as possible.



• *List of Voters.* This list contains all eligible voters for the given election. Depending on the scenario, the list may be open, i.e., the voters' identities are known, or protected, by anonymization techniques or by posting a condensed version of the list with Merkle trees, for example.

• *List of Candidates and Choices.* This list outlines the individual subjects on which voters must decide. Note that we use the word candidate as a generic term for all types of voting options.

• *List of Observers (Optional).* For some election events (e.g., nationwide governmental elections), the election officials may designate official observers whose responsibilities include the verification of the election event and mediation of disputes that might occur during the election. If observers are specified, their identifiers and associated public keys should be included.

• *Custom Parameters (Optional).* Other parameters may be added by election administrators based on an election's specific needs.

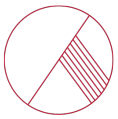
Once the election parameters are entered into the configuration file, officials generate a unique cryptographic identifier for the configuration file through a cryptographic hash function that can act as an ID representation of the election event. The officials also sign the configuration file with the identifier to prove that they are indeed the organizers of the election event. Once signed, the configuration file is stored on Agora's *Bulletin Board*.

Once the configuration file is posted on the *Bulletin Board*, it is available for public scrutiny. If the configuration file is accepted by the public and other interested parties, the system is ready for voters to proceed by casting votes.

STEP 2: CASTING

Once the casting phase has begun, each eligible voter (we will use female pronouns throughout this section) can begin submitting her vote in the election. A voter can access her "virtual" voting booth through a designated voting device, which allows her to fill out, review, seal (encrypt) and submit a ballot.

Agora allows voters to participate by using either their personal device, such as a smartphone or computer, or by using a voting machine at a traditional voting center operated by election officials. Regardless of which device the voter utilizes, its voting software fetches the election parameters from the *Bulletin Board* and enables the voter to complete a ballot. The voter then votes by selecting choices presented to her from the *Bulletin Board*. Once these selections have been made, the voter is ready to cast her ballot.



When the voter casts her ballot, it is encrypted by the voting software with the collective public key of the Cothority, which are the distributed Consensus Nodes of the Agora network. Agora's software utilizes the threshold ElGamal cryptosystem for encryption. To verify that an encrypted ballot still reflects the voter's choices, the software allows the voter to perform a Cast-as-Intended validation. There are two well-studied methods Agora intends to use that are primarily used to carry out Cast-as-Intended validations. [31, 61, 44, 22, 32]

Cast-or-Challenge Validation

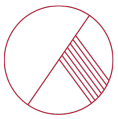
The concept of Cast-or-Challenge validation was introduced by Benaloh in 2006. [23] In this method, voters can test their voting device to ensure that it is encrypting data correctly. After sealing a ballot, the voter transmits her ballot to the *Bulletin Board* without her identity attached. Proof of proper encryption can be verified on a separate device called a voting assistant, [38] which reveals the relayed plaintext ballot. If the voting device's encryption is working property, the ballot will appear correctly on the voting assistant as well. Once encryption has been audited, a real ballot can then be cast. If Cast-or-Challenge validation is performed by a sufficiently large number of voters and auditors, the integrity of the vote casting step is ensured with high probability.

Code Voting Validation

Code Voting was first introduced by Chaum in 1991. [31] In Code Voting, election officials securely distribute a list of codes to the voters through a separate communication channel, usually via postal mail. Using the codes sent to them, voters can verify that the voting device correctly encrypted their choices by confirming that the codes displayed on the device match the codes received via postal mail. Since a malicious device would not know the mailed codes, this method makes it easy to determine whether a device is compromised.

Agora will utilize Cast-or-Challenge validation in our present implementation due to its simplicity (e.g., it does not require any action on the part of election administrators). However, since Code Voting validation provides stronger security guarantees, which is especially important in high-stakes elections, we intend to implement this method in the future as well. We will also evaluate the applicability of new techniques, such as Challenge-and-Cast validation, [39] which relies on zero-knowledge proofs.

Once the voting device's encryption is confirmed to be working properly, the voter casts her encrypted ballot by posting it to the *Bulletin Board* and signing the transaction with her digital identity credentials. The encrypted ballot is then received by one of the nodes in the Cothority and authenticated. Authenticated ballots are included in the *Bulletin Board*'s next Skipblock.



STEP 3: ANONYMIZATION

Every election system must guarantee the privacy of its voters. For Agora in particular, our system must ensure that votes cannot be linked to individual voters when votes are decrypted for tallying. In that respect, once the voting period ends, Agora's network runs all ballots through a mixing network to anonymize the encrypted ballots cast on the *Bulletin Board*.

A mixing network [33, 51] is a set of servers that sequentially re-encrypt a given dataset multiple times, where the correctness of each re-encryption is attested by zero-knowledge proofs. These correctness proofs are published to the *Bulletin Board* to enable auditability of this process. Only a single node in the network is required to behave honestly to ensure the protocol's correctness. Mixing networks' application to anonymous communication and digital voting have been studied extensively in the last decade, resulting in significant improvements in terms of security and performance. [33, 43, 51, 47, 34]

Agora intends to implement a Neff-shuffle-based [51] mixing network. We also plan to explore other encryption methods that are emerging, including Atom's butterfly mixing network [47] and bulletproofs, [28] a new mechanism for short zero-knowledge proofs that do not require trust.

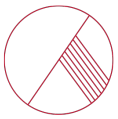
When ballots are sent through the mixing network, each mixing node processes the entire list of encrypted ballots and outputs a new list of anonymized ballots alongside zero knowledge proofs of proper shuffling to the *Bulletin Board*.

STEP 4: DECRYPTION

In order to perform the tallying process, the Cothority nodes will collectively decrypt the anonymized ballots and publish them with decryption correctness proofs onto the *Bulletin Board*.

To begin this process, Cothority nodes check that the zero-knowledge proofs from the anonymization phase are correct, and if so, the nodes begin to collectively decrypt the anonymized ballots. In this process, each Cothority node partially-decrypts each of the anonymized votes and generates a zero knowledge proof for each decryption, attesting to the correctness of the partial decryption. Once finished, all Cothority nodes publish their results to the *Bulletin Board*.

Election administrators can then check that the zero-knowledge proofs of the partially-decrypted ballots are correct. Provided that a sufficiently high threshold of them are valid, administrators can use the properly partially-decrypted ballots to recover the anonymized original plaintext ballots. The plaintext ballots are posted to the *Bulletin Board*, where they can be tallied.



STEP 5: TALLYING

After the decryption phase, Agora nodes tally votes across all valid decrypted ballots and publish the final results on the *Bulletin Board*.

Agora, election administrators or any third party overseeing the election can tally votes from the plaintext ballots posted on the *Bulletin Board* during the last phase. The party officially responsible for tallying votes posts the signed results to the *Bulletin Board*, at which point auditors can check the validity of the outcome before it is deemed to be final. When permitted, Agora will conduct an automated tally of votes, as well.

While the election administrator decides what party will be responsible for the official tally, anyone can tally votes in an election.

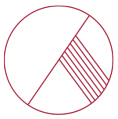
STEP 6: AUDITING

The ability to audit ballots and election results at every stage is one of the prime benefits to using Agora's platform. Our blockchain-based *Bulletin Board*, *Cotena* log and *Valeda* network are important elements of our system that enable enhanced auditing capabilities. Our auditing capabilities can be used by observers to validate *Bulletin Board* data.

Citizen Auditor Nodes can be election administrators, voters themselves or any third party. Once the election is tallied, the election's officially designated observers attest to the validity of an election by posting a signed statement on the Bulletin Board. Furthermore, anyone in the world can observe an election by running a Citizen Auditor Node. Auditor Nodes, which collectively form the Valeda network, validate cryptographic proofs to provide a decentralized and unbiased confirmation of election results. Agora provides many ways for people and organizations to act as an observer to elections on our platform, adding to its transparency.

To enable end-to-end verifiability for observers, all intermediate steps of the election process are third-party verifiable and are posted to the Bulletin Board. Specifically, an auditor or observer can run the following consistency checks:

- *Configuration:* Citizen Auditor Nodes confirm that election parameters are correct. Some observers may additionally have special rights granted by an election administrator that permits them to verify the relationship between the private credentials of voters and the public information posted on the *Bulletin Board*. Such officially-assigned observers can dramatically increase the transparency of an election.



• *Casting*: Citizen Auditor Nodes confirm that each encrypted ballot posted to the Bulletin Board is correctly tied to one of the authenticated voters specified in the configuration list. Depending on the validation mechanism, observers can also verify that ballot encryption worked properly and that it is in the proper format.

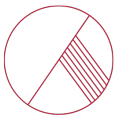
• *Anonymization*: Citizen Auditor Nodes confirm that all of the encrypted ballots on the Bulletin Board have been shuffled and anonymized properly. This includes checking all of the zero-knowledge proofs associated to every re-encryption step of the mix network.

• *Decryption*: Citizen Auditor Nodes ensure that all the partially-decrypted ballots are correct with respect to the corresponding zero-knowledge decryption proofs, and that the plaintext votes are correctly reconstructed from the partially-decrypted ballots.

• *Tallying*: Citizen Auditor Nodes confirm that the final election results are correctly computed from the plaintext votes.

If the election process is successfully verified according to the official observer, a final attestation is signed with the observer's private key. It is unforgeable under general cryptographic assumptions and provides additional public proof that can be verified by anyone. This final signature can be especially powerful when the official observer is a widely-recognized trusted and unbiased party.

All voters and third-party observers will be able to audit the election process through Agora's software, which will act as an Agora blockchain explorer with audit tools. A selection of Citizen Auditor Nodes will record the output of their proofs on the Bulletin Board.



4.2. DIGITAL IDENTITIES

A challenge in any election event revolves around the validation of voter identities and voting eligibility. Even in traditional paper-based voting systems, it can be difficult to identify that voters are who they claim to be. For example, some ineligible voters have been allowed to cast votes remotely by registering under the names of deceased individuals [60]. In the digital context, the verification of a voter is fundamentally more challenging due to ongoing limitations around securely binding physical and digital identities.

In that respect, Agora relies on voting administrators to select an identity management system and provide a mechanism to authenticate voters. At the same time, Agora intends to work with digital identity providers to provide governments and institutions with digital identity solutions compatible with Agora's voting system. We will place an emphasis on investigating solutions compatible with the latest advances in digital identity technology, notably decentralized and sovereign identity solutions such as uPort [48] and Civic. [57]

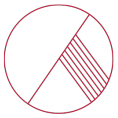
4.3. DISPUTE RESOLUTION

While we endeavor to automate as much of the election process as possible, many things can go wrong. For example, an eligible voter in the identity management system may not be not registered on the configuration list. In cases such as this where no algorithmic, deterministic decision is satisfactory, human intervention is required.

4.3.1. ROLE OF AUDITORS

Election administrators are advised to designate official auditors to mediate issues that arise. Countries such as Cambodia and Libera have solicited the presence of the U.N. [35] and the Carter Center [30] to be observers of their elections, testifying to the validity of the election process and mitigating conflicts. On Agora's platform, these official auditors are listed in the configuration file parameters. These auditors can be called upon in case of conflicts or issues during the event to act as third party mitigators.

Organizations that would be viewed as likely auditors include non-governmental organizations advocating for civil and political rights, intergovernmental organizations, independent institutions dedicated to education or research (such as universities and foundations) and recognized auditing firms. All selected organizations will be expected to be sufficiently knowledgeable in digital and blockchain voting observation.



4.3.2. DISPUTES

Auditors, voters or other third parties may detect issues during an election. Agora intends to build mechanisms to report anomalies to the auditors as well as Agora in a user-friendly and secure way. For each report made, a proof of report will be provided to confirm that the issue has been submitted to the auditors and Agora. As with traditional voting systems, conflicts will be resolved in accordance to each jurisdiction's individual election rules and laws.

If auditors are to be the mediators in an election, several solutions exist. The simplest way to mediate disputes is to grant power to one auditor or organization. However, more sophisticated solutions can be used to create a more credible dispute resolution mechanisms. For example, several auditors may be authorized to vote on disputes, and the outcome will depend on whether a pre-defined threshold of the auditors agree on a resolution. Agora intends to introduce new dispute resolution mechanisms over time for the jurisdictions we serve.

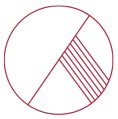
4.3.3. AUDITOR AUTHENTICATION

When auditors resolve a dispute, their resolution should be published to the *Bulletin Board* and signed with their private key. In the case of an eligible voter that needs to be added to the configuration file, the auditor can report the identity of the new voter to be added in a signed message to Agora, which our platform can then use to automatically add the individual as a valid voter in the *Bulletin Board*.

In many elections, governments may require that traditional judicial measures be taken. Agora and the auditors in the election will act in accordance with the laws of our election jurisdictions. Agora will also strive to follow best practices on election dispute resolutions set forth by the international community whenever possible (U.N., Carter Center, etc.). [29, 21, 55]

4.4. ABSENTEE BALLOTS

Agora's technology also provides ways to cast absentee ballots, which are utilized for voting when an individual is outside of her voting jurisdiction or is unable to visit a prescribed in-person voting location.



4.5. SYSTEM PROPERTIES

There are various requirements we set out to fulfill in the architecture of Agora's blockchain-based platform. We believe these items are important to the creation of a fair and transparent voting system. Our goals include end-to-end verifiability, voter privacy and more, which are explained in the sections below.

4.5.1. END-TO-END VERIFIABILITY

In order to ensure full transparency, interested parties must be able to audit both our technology and all aspects of the elections held on Agora's technology. The following properties ensure that any interested party, be it a voter, election official or auditor, is able to verify the validity of the voting process:

- *Validation.* Voters can verify that their ballot is encrypted properly and that their votes are being cast as intended. Cast-or-Challenge and Cast-as-Intended are two types of validation that can be utilized to ensure votes are correctly recorded by the system.

- *Collected-as-Cast Validation.* Voters can independently verify that their vote has been correctly recorded.

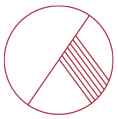
- *Tallied-as-Collected Validation.* Anyone can verify that every collected vote is correctly included in the complete election tally.

- *Voter Eligibility Validation.* Anyone can review the list of eligible voters.

4.5.2. VOTER PRIVACY

Ensuring that an individual's vote is kept private is crucially important to maintaining a fair election process. When voters feel coerced to vote differently from their true preferences, election results cannot be said to reflect the legitimate will of the voters. Agora maintains voter privacy in the following ways:

- *Voter Anonymity.* It is not possible to determine which of the eligible voters cast any particular vote, except with negligible probability.



• *Vote Secrecy.* It is not possible to determine the vote any given voter has cast, except with negligible probability.

• *Receipt Freedom.* Voters cannot prove to any third parties how they voted.

4.5.3. OTHER GOALS

We have mandated that Agora's technology fulfill several other requirements. These additional requirements include:

• *No Single Points of Failure.* The system is decentralized and able to function correctly even in the presence of a limited number of Byzantine faults.

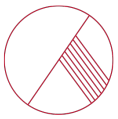
• *Availability.* The probability that the system is non-operational at any given time is negligible.

• *Usability.* Any non-technical voter must be able to cast and verify his or her vote with a negligible error rate.

• *Offline Verifiability.* To verify voting information and audit the election on any individual device, no active communication is necessary after the election data has been downloaded from the *Bulletin Board*.

• *Regulatory Adaptability.* The system must be adaptable to given jurisdictional requirements.

We have implemented these goals into our blockchain-based technology in order to offer fully-transparent and fair elections.



REFERENCES

[1] Esteve, J. i, Goldsmith, B., & Turner, J. (2012). International Experience with E-Voting Norwegian E-Vote Project, (June), p.78. Retrieved from http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf%5Cnhttp://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf%5Cnhttp://216.65.11

[2] King, C., & Thompson, M. (2002). Security of Electronic Voting in the US, p.4.

[3] Selker, T., & Cohen, S. (2005). An Active Approach to Voting Verification. Caltech / Mit Voting Technology Project " Threats To Voting Systems " Workshop, p.3.

[4] Fischer, E.: Election reform and electronic voting systems: analysis of security issues In: CRS Report for Congress No. RL32139. Congressional Research Service, Washington, D.C. (2003), p.12. https://epic.org/privacy/voting/crsreport.pdf

[5] Esteve, J. i, Goldsmith, B., & Turner, J. (2012). International Experience with E-Voting Norwegian E-Vote Project, (June), p. 96. Retrieved from http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf%5Cnhttp://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf%5Cnhttp://216.65.11

[6] Johnson, N., Jones, B. M., & Clendenon, K. (2017). e-Voting in America: Current Realities and Future Directions. In G. Meiselwitz (Ed.), Social Computing and Social Media. Human Behavior (pp. 337–349). Cham: Springer International Publishing.

[7] Carrier, M. (2005). Vote counting, technology, and unintended consequences. St John's Law Review, 79(3), p. 664. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stjohn79&section=29

[8] Brennan, T. H. E., Technology, V., Project, A., Norden, L., Rights, V., Series, E., & Justice, F. O. R. (2006). The machinery of democracy: Voting System Security, Accessibility, Usability, and Cost, p.138.

[9] Norden, L., & Famighetti, C. (2015). America's Voting Machines at Risk, p.8. Retrieved from https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf

[10] https://www.interieur.gouv.fr/Publications/Rapports-de-l-IGA/Elections/Revue-de-depenses-rapport-sur-l-organisation-des-elections

[11] http://www.elpais.com.co/economia/enterese-de-cuanto-le-cuestan-las-elecciones-a-los-colombianos.html

[12] http://time.com/money/4556642/election-day-2016-costs-country-voters/

[13] https://webrootsdemocracy.files.wordpress.com/2017/11/cost-of-voting-webroots-democracy.pdf

[14] http://news.bbc.co.uk/2/hi/africa/7178393.stm

[15] https://www.standardmedia.co.ke/article/2000228493/election-related-violence-the-biggest-worry-for-kenyans-in-2017

[16] Calingaert, D. (2006). Election Rigging and How to Fight It. Journal of Democracy, 17(3), p.138. http://doi.org/10.1353/jod.2006.0043

[17] Goggin, S. N., Byrne, M. D., & Gilbert, J. E. (2012). Post-Election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence. Election Law Journal: Rules, Politics, and Policy, 11(1), p.46. http://doi.org/10.1089/elj.2010.0098

[18] http://politicalticker.blogs.cnn.com/2013/03/28/obama-to-form-commission-on-long-lines-to-vote/

[19] http://en.interfax.com.ua/news/general/233548.html

[20] https://en.wikipedia.org/wiki/Skip_list

[21] ace project. Electoral dispute resolution. http://aceproject.org/ace-en/topics/lf/lfb12/default , 2017. [22] Adida B. Helios: Web-based open-audit voting. In USENIX security symposium 2008 Jul 28 (Vol. 17, pp. 335-348), 2008.

[23] Josh Benaloh. Simple verifiable elections. In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, EVT'06, pages 5–5, Berkeley, CA, USA, 2006. USENIX Association.

[24] Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L.Vora, and Dan S.Wallach. Public Evidence from Secret Ballots, pages 84–109. Springer International Publishing, Cham, 2017.

[25] Dan Boneh. The decision diffie-hellman problem. Algorithmic number theory, pages 48–63, 1998. [26] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, and Bryan Ford. Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies. In 1st IEEE Security and Privacy On The Blockchain, April 2017.

[27] Joppe W Bos,J Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. Elliptic curve cryptography in practice. In International Conference on Financial Cryptography and Data Security, pages 157–175. Springer, 2014.

[28] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Efficient range proofs for confidential transactions. Cryptology ePrint Archive, Report 2017/1066, 2017. https://eprint.iacr.org/2017/1066.

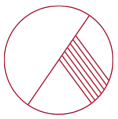
[29] Carter Center. Guide to electoral dispute resolution. https://www.cartercenter.org/resources/ pdfs/news/peace_publications/conflict_resolution/election-dispute-guide.pdf , 2010.

[30] Carter Center. Waging peace through elections. https://www.cartercenter.org/peace/democracy/ observed.html , 2017.

[31] D. Chaum. Surevote: Technical overview. In IAVoSS Workshop on Trustworthy Elections, WOTE 01, 2001.

[32] David Chaum, Richard T Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L Rivest, Peter YA Ryan, Emily Shen, Alan T Sherman, and Poorvi L Vora. Scantegrity ii: End-to-end verifiability by voters of optical scan elections through confirmation codes. IEEE transactions on information forensics and security, 4(4):611–627, 2009.

[33] David L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84–90, 1981.



[34] George Danezis. Mix-networks with restricted routes. Springer.

[35] DPA, DPKO, UNDP, OHCHR, UNV, UNOPS, and UNESCO. Observation and assistance in worldwide elections. http://www.un.org/undpa/en/elections , 2017.

[36] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4):469–472, 1985.

[37] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In GeorgeBlakleyandDavidChaum,editors, Advances in Cryptology, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 1985.

[38] Dawid Gaweł, Maciej Kosarzecki, Poorvi L. Vora, Hua Wu, and Filip Zagórski. Apollo – End-to-End Verifiable Internet Voting with Recovery from Vote Manipulation, pages 125–143. Springer International Publishing, Cham, 2017.

[39] Sandra Guasch1 and Paz Morillo2. How to challenge and cast your e-vote.

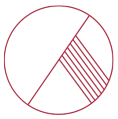
[40] Rolf Haenni, Reto E. Koenig, and Eric Dubuis. Cast-as-Intended Verification in Electronic Elections Based on Oblivious Transfer. In Electronic Voting: First International Joint Conference, E-Vote-ID 2016, October 2016.

[41] Rolf Haenni, Reto E. Koenig, Philipp Locher, and Eric Dubuis. Chvote system specification. Cryptology ePrint Archive, Report 2017/325, 2017. http://eprint.iacr.org/2017/325 .

[42] S. Hauser and R. Haenni. Implementing broadcast channels with memory for electronic voting systems. In JeDEM eJournal of eDemocracy and Open Government, 8(3):6179, 2016, 2016.

[43] Markus Jakobsson, Ari Juels, and Ronald L. Rivest. Making mix nets robust for electronic voting by randomized partial checking. In Proceedings of the 11th USENIX Security Symposium, pages 339–353, Berkeley, CA, USA, 2002. USENIX Association.

[44] Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira. Veryvote: A voter verifiable code voting system. In Proceedings of the 2Nd International Conference on E-Voting and Identity, VOTE-ID '09, pages 106–121, Berlin, Heidelberg, 2009. Springer-Verlag.



[45] Aniket Kate and Ian Goldberg. Distributed key generation for the internet. In Distributed Computing Systems, 2009. ICDCS'09. 29th IEEE International Conference on, pages 119–128. IEEE, 2009.

[46] Katzenpost. https://katzenpost.mixnetworks.org/.

[47] Albert Kwon, Henry Corrigan-Gibbs, Srinivas Devadas, and Bryan Ford. Atom: Scalable anonymity resistant to traffic analysis. CoRR, abs/1612.07841, 2016.

[48] Dr. Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. Uport: A platform for self-sovereign identity, 2017.

[49] Alfred J. Menezes and Scott A. Vanstone. Elliptic curve cryptosystems and their implementation. Journal of Cryptology, 6:209–224, 1993.

[50] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[51] C Andrew Neff. A verifiable secret shuffle and its application to e-voting. In Proceedings of the 8th ACM conference on Computer and Communications Security, pages 116–125. ACM, 2001.

[52] Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, and Bryan Ford. CHAINIAC: Proactive software-update transparency via collectively signed skipchains and verified builds. In 26th USENIX Security Symposium (USENIX Security 17), pages 1271–1287, Vancouver, BC, 2017. USENIX Association.

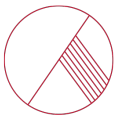
[53] nVotes. Multiplicative vs additive homomorphic elgamal. 2016.

[54] Torben P Pedersen et al. Non-interactive and information-theoretic secure verifiable secret sharing. Springer.

[55] Denis Petit. Resolving election disputes: Towards a standard election dispute monitoring system. http://www.osce.org/odihr/elections/17567?download=true , 2000.

[56] Victor Shoup and Rosario Gennaro. Securing threshold cryptosystems against chosen ciphertext attack. Advances in Cryptology EUROCRYPT'98, pages 1–16, 1998.

[57] Civic team. Civic, 2017.



[58] Alin Tomescu and Srini Devadas. Catena: Efficient Non-equivocation via Bitcoin. In 38th IEEE Symposium on Security and Privacy, pages 393–409, May 2017.

[59] Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 2014.

[90] NBC New York. More than 200 dead people shown to have voted in ny county elections: Report. https://www.nbcnewyork.com/news/local/Dead-Voter-List-Long-Island-Nassau-County-Newsday-230030371.html , 2013.

[61] Filip Zagórski, Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, and Poorvi L. Vora. Remotegrity: Design and use of an end-to-end verifiable remote voting system. In Proceedings of the 11th International Conference on Applied Cryptography and Network Security, ACNS'13, pages 441–457, Berlin, Heidelberg, 2013. Springer-Verlag.