# 1. Use Case Description:

The use case revolves around the development of a voting platform named "BitVote," which focuses on providing organizations with a secure and transparent voting system. The platform's primary objective is to ensure that the voting processes are conducted in a manner that is both secure and transparent. BitVote allows organizations to establish voting pools, enabling users to vote securely and anonymously.

To enhance security and control, the platform incorporates access controls and customizable features for pool creation. For example, organizations can set deadlines for pool closure, allowing for efficient management of the voting process. These customizable options provide flexibility and adaptability to meet the specific requirements of each organization's elections.

By leveraging blockchain technology, BitVote ensures the immutability and transparency of the voting process. Blockchain serves as a decentralized and tamper-resistant ledger, recording each vote in a transparent and permanent manner. This feature instills confidence in the integrity of the voting system. Additionally, the utilization of blockchain technology allows for the maintenance of voters' privacy and security.

The ultimate goal of BitVote is to create a user-friendly and straightforward application that facilitates secure and transparent voting. The platform seeks to provide an intuitive interface that simplifies the voting process for users, ensuring a positive and accessible experience. Through the combination of security, transparency, privacy, and user-friendliness, BitVote aims to contribute to the advancement of democratic processes and trustworthy elections.

# 2. Data and Transaction Model:

## 2.1 Modeling Participants, Assets, and Transactions:

In the BitVote platform, various entities are modeled to ensure the smooth functioning of the voting system:

* **Participants**: This entity encompasses different individuals and organizations involved in the voting process. It includes registered voters, organizations hosting the elections, and administrators responsible for managing the platform. Each participant is uniquely identified within the blockchain network through a specific address or identifier. These addresses serve as a way to authenticate and track the actions of participants on the platform.
* **Assets**: The platform revolves around the primary asset, which is the vote itself. Each vote is associated with a specific voter and a particular voting poll. The vote is a critical component that reflects the preference or choice of the voter. Additionally, other assets may exist within the system to facilitate authorization or access control. These assets could be in the form of tokens that participants hold to verify their eligibility to participate in specific voting pools or to access certain functionalities within the platform.
* **Transactions**: Transactions form the core interactions within the BitVote platform. The primary transaction is the vote submission transaction, where a registered voter submits their vote to a specific voting pool. This transaction is crucial for recording and processing the votes securely and transparently. Other types of transactions may include pool creation, allowing organizations to establish new voting pools, pool closure to signify the end of a voting period, and various administrative actions performed by authorized administrators. These transactions ensure the proper management and operation of the platform.

By modeling participants, assets, and transactions within the BitVote platform, the system can effectively capture the involvement of various stakeholders, manage the crucial asset of votes, and enable necessary interactions to facilitate secure and transparent voting processes.

# 3. Logic (Smart Contracts):

## 3.1 Business Rules:

The following business rules govern the BitVote platform:

* Each user can participate in multiple voting pools.
* Each voting pool has a specific set of eligible voters.
* A user can submit only one vote per voting pool.
* Voting polls can have customizable options, such as closure deadlines and access controls.
* Only authorised administrators can create and manage voting pools.

## 3.2 Types of Events and Event Consumers:

Within the BitVote platform, different types of events are generated to capture important actions and updates:

* **VoteSubmissionEvent**: This event is generated when a user successfully submits their vote to a specific voting pool. It contains essential information such as the address or identifier of the voter, the identifier of the voting pool, and the chosen vote. This event allows for the tracking and recording of individual votes, ensuring transparency and accountability.
* **PoolCreationEvent**: This event is generated when an administrator successfully creates a new voting pool within the platform. It includes details about the pool, such as the pool identifier, access controls defining who can participate, and the deadline for pool closure. This event provides a record of the creation of new voting pools and their associated parameters.

Event consumers within the BitVote platform can include:

* **Frontend applications**: Frontend applications can consume these events to provide real-time updates to users. For example, when a VoteSubmissionEvent occurs, the frontend application can update the user interface to display a confirmation message or provide a notification to the voter about the successful submission of their vote. Similarly, when a PoolCreationEvent takes place, the frontend application can dynamically update the available voting options or display information about the newly created pool.
* **Backend systems:** Backend systems within the BitVote platform can consume these events for various purposes. They can utilize the events for auditing and logging, maintaining a comprehensive record of vote submissions and pool creations. These events can also trigger further actions or workflows within the backend systems. For instance, a PoolCreationEvent might trigger the generation of reports or the initiation of background processes for data analysis or verification purposes.

# 4. Privacy and Security:

## 4.1 Authentication and Authorization:

The BitVote platform places a strong emphasis on privacy and security, employing authentication and authorization mechanisms to safeguard the integrity of the voting process:

* **Authentication**: To ensure that only authorized participants can engage with the platform, authentication is enforced. Participants are required to authenticate themselves using their unique addresses or identifiers within the blockchain network. These addresses serve as a form of digital identity and provide a means to verify the legitimacy of participants. By authenticating with their unique identifiers, participants establish their identity and gain access to the functionalities of the BitVote platform.
* **Authorization**: Access controls play a crucial role in maintaining the security of the platform. BitVote implements authorization mechanisms to determine which participants are eligible to join specific voting pools. These access controls ensure that only individuals who meet the predefined criteria or possess the necessary permissions can participate in particular voting pools. This ensures that only authorized voters can cast their votes in relevant elections or decision-making processes.

Administrators, as privileged users within the system, are granted additional authorization privileges. They have the authority to create and manage voting pools. This includes defining the access controls for each pool and configuring the pool closure deadlines. By granting administrators specific authorization privileges, the BitVote platform enables effective management of voting pools while maintaining security and control over the voting process.

# 5. Integration:

## 5.1 Interaction with External Systems:

The BitVote blockchain network offers the capability to interact with external systems through calls and events, allowing for seamless integration and information exchange:

* **Calls**: External systems have the ability to make calls to the BitVote blockchain network to retrieve specific information. These calls can be utilized by frontend applications or backend systems to access data about voting pools, participants, or voting results. For example, a frontend application may make a call to retrieve the current status of a voting pool, displaying the number of votes cast or the deadline for pool closure. Similarly, a backend system may make calls to gather aggregated voting data for generating reports or conducting further analysis. These calls facilitate the integration of the blockchain network with external systems, enabling the retrieval of relevant information for various purposes.
* **Events**: The BitVote blockchain network is capable of emitting events that external systems can consume. Events are triggered by specific actions or transactions within the blockchain network and provide real-time updates to external systems. For instance, when a vote is submitted or a voting pool is created, corresponding events can be emitted. External systems, such as frontend applications or backend systems, can subscribe to these events and receive notifications in real-time. This allows for immediate updates and integration with external systems. External systems can utilize these events for various purposes, such as generating reports based on the latest voting activities or triggering additional actions based on specific events.

# 6. Architecture Organization:

## 6.1 Peers and Organizations:

The BitVote platform is composed of two key components: peers and organizations, which work together to ensure the proper functioning of the blockchain network:

* **Peers**: Peers are individual nodes within the BitVote blockchain network. They play a vital role in the consensus and endorsement processes. Consensus refers to the mechanism by which peers collectively agree on the validity of transactions and the order in which they are added to the blockchain. Peers work together to maintain a distributed and synchronized ledger, ensuring the immutability and integrity of the voting data. Additionally, peers execute smart contracts, which are self-executing contracts with predefined rules encoded within the blockchain. These smart contracts automate certain actions within the BitVote platform, such as vote submission and verification. By collectively participating in consensus and executing smart contracts, peers contribute to the secure and transparent operation of the BitVote platform.
* **Organizations**: Organizations represent unique entities within the BitVote ecosystem. They can include the platform provider, participating organizations hosting elections, and administrative bodies overseeing the voting process. Each organization may have one or more peers associated with it. These organizations define and enforce specific rules, access controls, and governance policies within their respective domains. For example, the platform provider organization may establish the overall governance framework for the BitVote platform, while participating organizations create and manage individual voting pools for specific elections. By organizing entities into distinct organizations, the BitVote platform enables the delineation of responsibilities and permissions, promoting efficient management and administration of the platform.

## 6.2 Consensus/Endorsement Mechanism:

The BitVote network employs consensus and endorsement mechanisms to establish the integrity and immutability of the voting process:

* **Consensus**: The BitVote blockchain network relies on a consensus mechanism, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), to achieve agreement among the participating peers on the ordering and validity of transactions. Consensus is crucial to ensure that all peers within the network have a shared and consistent view of the blockchain's state. In a PoW consensus mechanism, peers compete to solve complex mathematical problems to validate transactions and add them to the blockchain. In a PoS consensus mechanism, peers with a significant stake in the network are selected to validate transactions based on their ownership and participation. By reaching consensus, BitVote ensures that all peers agree on the order and validity of voting transactions, maintaining a consistent and trustworthy record of votes.
* **Endorsement**: Within the context of smart contracts in BitVote, endorsement refers to the process of validating and executing transactions. Peers within the network endorse transactions based on rules and criteria set by the smart contract. Endorsement ensures that transactions comply with the specified conditions and requirements before they are added to the blockchain. By endorsing transactions, peers verify their correctness, authenticity, and compliance with the smart contract logic. This validation process helps to maintain the integrity of the voting process by ensuring that only valid and authorized transactions are included in the blockchain.

# 7. Network hosting

What is the chosen hosting strategy?

# 8. Individual contribution table

A table containing a description of the contribution per participant. Students should inform which task they were responsible for. Evidence and explanations of the activity are mandatory.

| Bruno Marques | Task | Evidence | Explanation |
| --- | --- | --- | --- |

| Wietze Bronkema | Task | Evidence | Explanation |
| --- | --- | --- | --- |

| Sander Harks | Task | Evidence | Explanation |
| --- | --- | --- | --- |

| Mike Fels | Task | Evidence | Explanation |
| --- | --- | --- | --- |

# 9. Repository

<https://github.com/brumarq/bitvote>

Checkout the readme.md file for installation and usage instructions