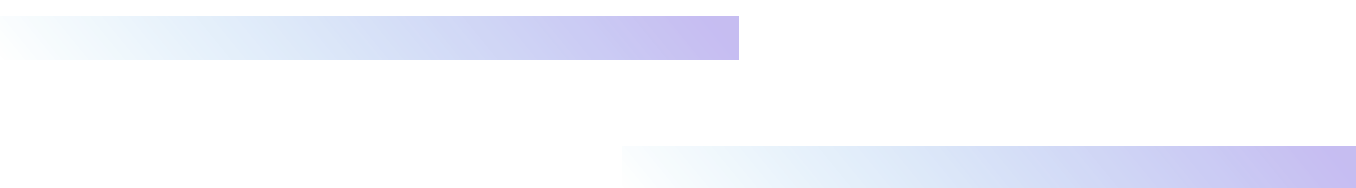




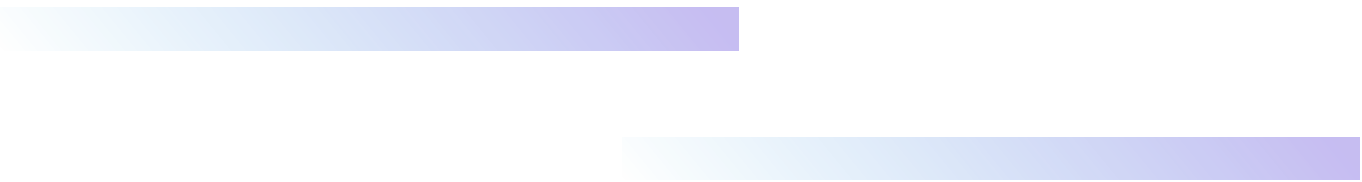
ELECTUS

THE EVOLUTION OF GOVERNANCE



CONTENTS

The Problem	03
Protocol	06
What is Electus Protocol	07
Understanding Entities	12
Understanding Polls	14
Understanding Actions	17
Products	20
Vault	21
Stream	25
Polis	28
Other Potential Use Cases	34
Governance of Protocol	36
Team	42





THE PROBLEM

GOVERNANCE, MEMBERSHIP, AND COMPLIANCE

The above stated problems are intrinsic to the society itself; that we as humankind have been tackling since ages successfully to scale up as a society in the first place.

Consider a few examples like driver licences, senates, financial compliance and similar other permissioning systems. Cooperating with each other as a society would be nothing less than chaotic.

In fact, one common phrase used to denote chaos, 'the wild west', is derived from what was an inevitable consequence of the lack of such systems in the newly annexed parts of USA in 1865-1895. There is no denying that without such systems, our world today would be a wild west.

CENTRALISATION & CONCENTRATION OF POWER

The current system in place to tackle the above problems end up concentrating a lot of power in the hands of individuals who may be apathetic at best, and unscrupulous at worst.

These systems are not transparent, and require frequent, direct action from the arbiters of the systems. As a result, sometimes they are unreliable, and sometimes they end up being very costly and time consuming.

Distributed ledgers, specifically blockchains present an opportunity to redesign these systems to make them more transparent, accountable, and reliable.

The Electus Protocol is an attempt to standardize governance applications built on blockchain.

TRUSTLESSNESS-USABILITY TRADEOFF

Blockchains so far have mostly been used to create unprecedented applications that are permissionless, trustless and absolutely eliminate rent-seeking intermediaries.

However, the problems described in the previous slide, while can leverage aspects of the blockchain like transparency and immutability, are by nature, permissioned. As a result, we have to move one step away from trustlessness in order to expand the scope of applications that the blockchain can disrupt.

That being said, the Electus Protocol introduces ways to carry out governance with the trusted party, that minimizes the role of the trusted party. This makes these systems cheaper, faster, more reliable and much more accessible. In essence, the remainder of this document will describe a protocol that standardizes membership, permissioning and voting systems on the blockchain.



PROTOCOL

*WHAT IS
ELECTUS PROTOCOL?*

THE ABSTRACT

Our protocol allows for the implementation of a standard API for Membership Verification Token within smart contracts. This standard provides basic functionality to track membership of individuals in certain on-chain 'organizations'. This allows for several use cases like automated compliance, and several forms of governance and membership structures.

We considered use cases of MVTs being assigned to individuals which are non-transferable and revocable by the owner. MVTs can represent proof of recognition, proof of membership, proof of right-to-vote and several such otherwise abstract concepts on the blockchain.

In general, an individual can have different memberships in his day to day life. The protocol allows for the creation of software that puts everything all at one place. His identity can be verified instantly. Imagine a world where you don't need to carry a wallet full of identity cards (Passport, gym membership, SSN, Company ID etc) and organizations can easily keep track of all its members. Organizations can easily identify and disallow fake identities.

LET US TALK ABOUT THE NOMENCLATURE FIRST

Entity:

The entity is a smart contract designed to track membership. It is operated by the contract owner, called the admin. The entity contains information about which ethereum addresses are part of the governance unit.

Poll:

A poll is a smart contract designed to track votes of people belonging to a certain entity, or combination of entities. The poll contains information about what the governance unit wishes for in a certain matter.

Action:

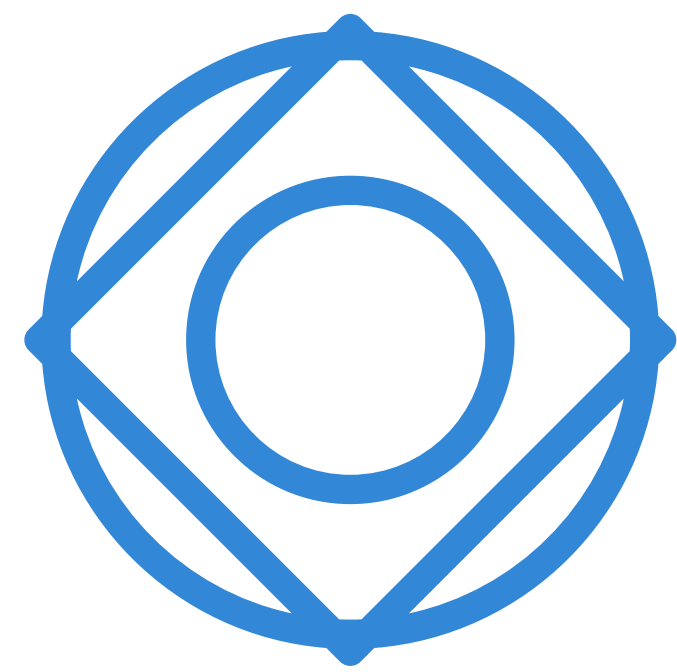
An action is a smart contract which can be triggered to take certain action or execute a strategy based on the result of a poll. They are triggered by transactions and carry out the instructions in a 'code is law' fashion.

THE E.P.A. FRAMEWORK

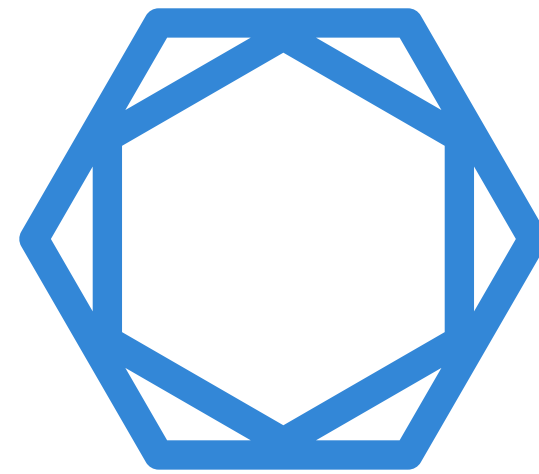
Entities, polls, and actions collectively are building blocks for any governance structure that one would want to build on top of a smart contract platform. The entity decides who governs, the poll records what they want, and the action carries out the premeditated, agreed upon tasks.

As a result, action contracts take up information from relevant poll contracts, and poll contracts take up relevant information from the entity contract. Action contracts can also directly take up information from an entity contract to represent action based on membership as opposed to action based on consensus when it takes up information from a poll.

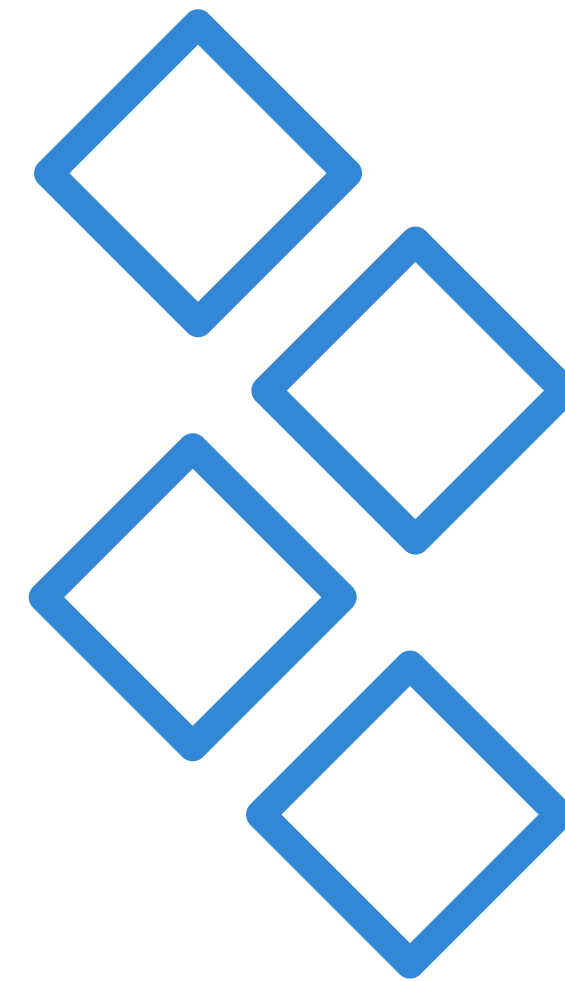
HOW THE E.P.A. FRAMEWORK FUNCTIONS?



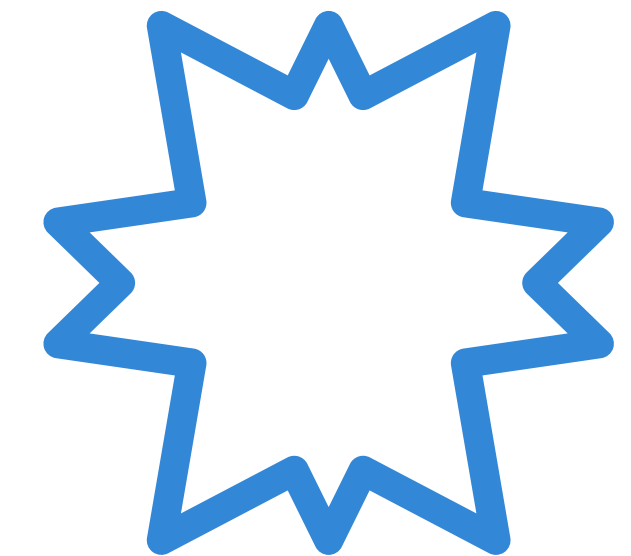
Entity Contract



Polls



Member Votes



**Action Contract
Activation**

UNDERSTANDING ENTITIES

Signatures

Photographer's Signature

WHAT IS AN ENTITY?

An entity is a contract which uses non transferable, revocable, boolean quantity tokens to mark ethereum addresses as members. The contract owner can use assign and revoke functions of the contract to add and remove members from the entity. Contract allows for instantly checking whether a certain address is or isn't a member of a certain entity. Different members of the same entity are not distinguishable on the blockchain. This hides the identity of a user while affirming their membership.

WHO CAN BE AN ENTITY?

Any organization which functions on the basis of a membership can use an entity to carry out its membership management.

Examples: *library , citizenship , voter authentication , investor accreditation vendor , stock issuer wanting to vet it's investors.*

UNDERSTANDING POLLS

HOW ARE THEY RELATED TO AN ENTITY?

Polls aggregate voting information based on 2 things.

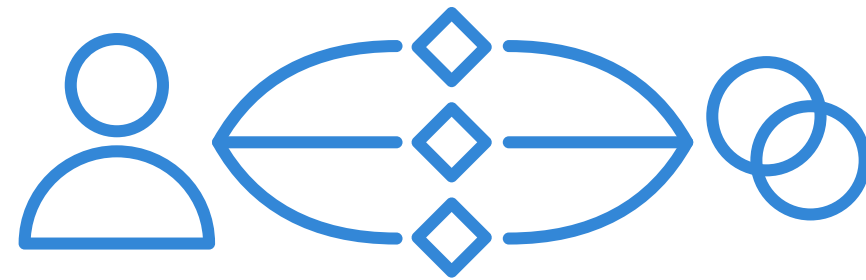
A) Whether or not the voter is a member of a specific entity or combination of entities, for example: must be a member of entity X and not a member of entity Y.

B) A vote weightage policy, for example: proportional to some token balance, or proportional to time locked tokens, or delegated democracy etc.

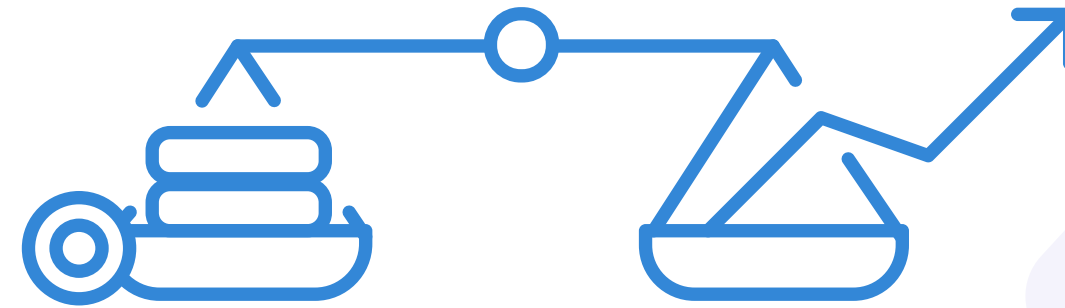
Polls can also be divided into time bound or time unbound polls. Bound polls stop recording votes after a certain time while unbound polls continually record votes with no time bound.

KINDS OF POLLS

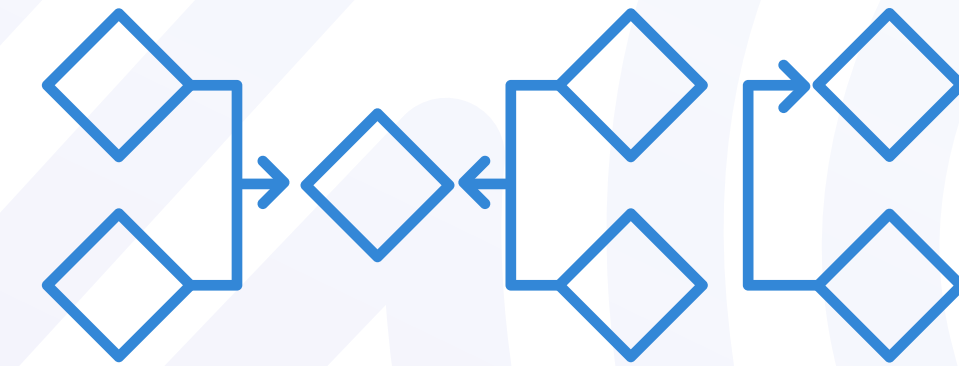
There is no limit to the kind of vote weightage policy, so several kinds of polls can be made. Some examples which illustrate this fact:



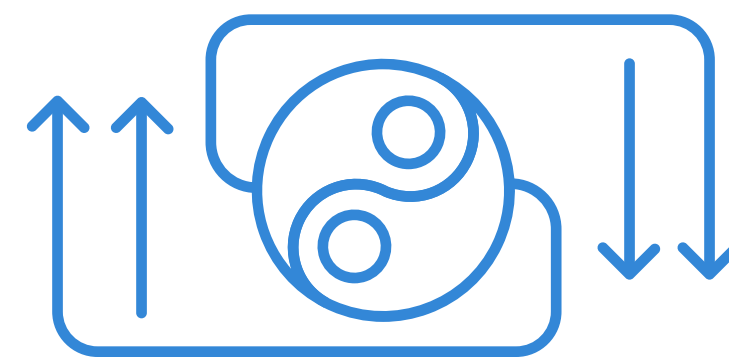
One person - One Vote



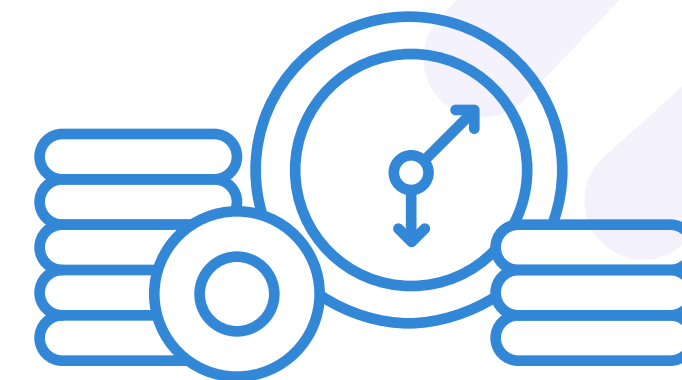
Token Weighted



Delegated Voting



Karma Voting



Token x Stake Time

UNDERSTANDING ACTIONS

HOW ARE THEY RELATED TO POLLS?

Actions carry out certain pre decided tasks based on the outcome of consensus, or a combination of such outcomes. Hence, it is crucial for these contracts to be linked with the polls that are relevant to it.

Some examples of poll driven actions are:

- A) Tap increment on a daico contract
- B) Re-electing the admin of an entity contract

ARE POLLS NECESSARY?

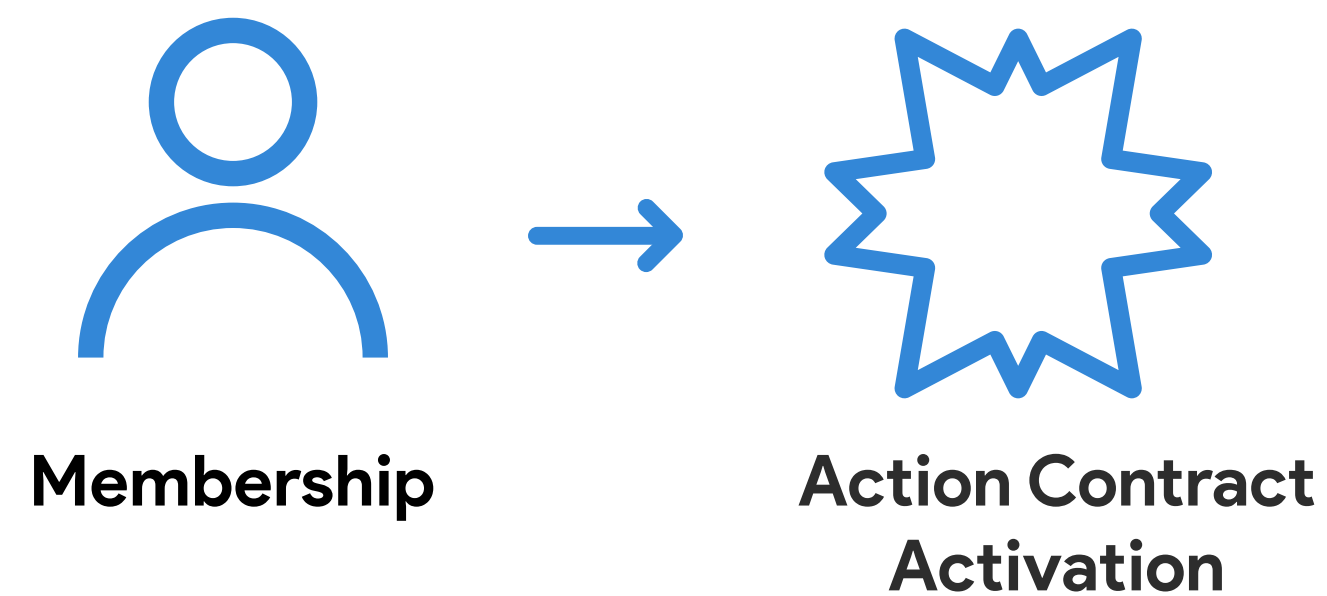
It is possible for actions to seek information directly from the entity as opposed to polls. Actions taking messages from polls are Action Based on Consensus type(ABC), and actions reading directly from entities are Action Based on Membership type(ABM).

ENTITIES FOR PERMISSIONING

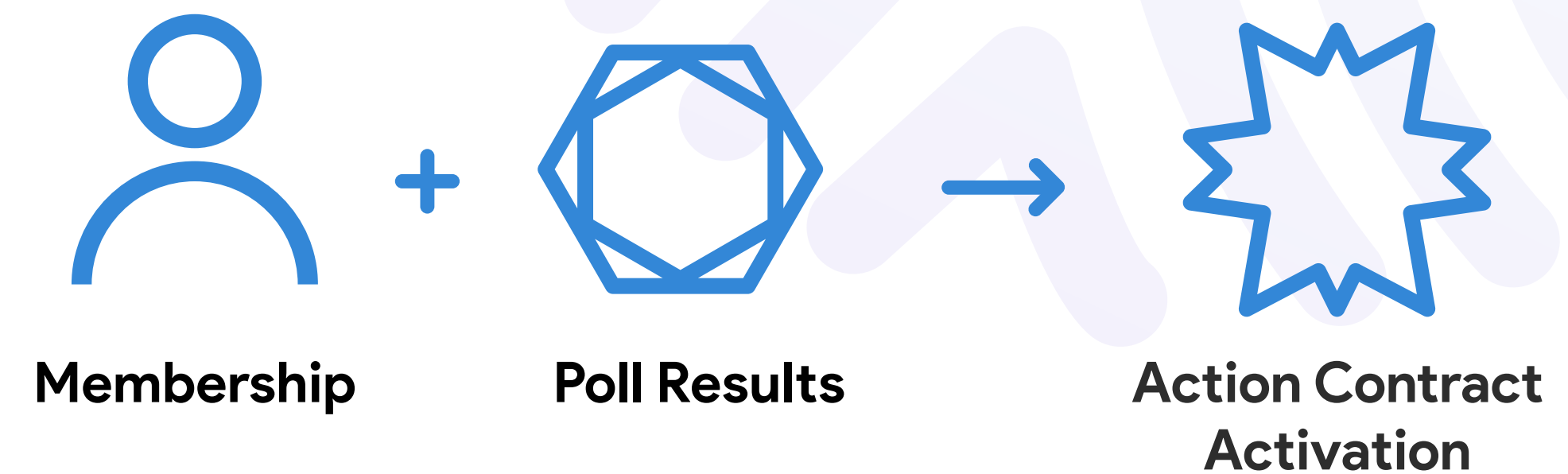
ABM contracts are useful in systems that need to deliver compliance as a service.

Security tokens should only be held by accredited investors. This problem is solved by making the accredited investors members of an entity and writing the ABM functionality into the code of the security token itself.

ABM ACTION CONTRACTS



ABC ACTION CONTRACTS





PRODUCTS

PRODUCT ONE
VAULT



WHAT'S A DAICO*?

ICO space is like the wild west. Investors need more control over contributed funds. These controls can be implemented via tap increment policies and contract kill policies.

Investors vote for or against motions to refund the money, increase cash flow, etc.

- A) Fund raising entity has to act responsibly
- B) Contract cannot be choked from an attack

USING THE PROTOCOL TO FACILITATE MEMBERSHIP

- ◆ Vault is an entity whose membership allows investors and issuers to take part in an ecosystem of DAICOs .
- ◆ Membership to Vault is based upon KYC, in order to check that one person has only one voting address.
- ◆ The membership system is powered by the electus protocol, wherein the DAICO polls and actions are building blocks of the platform and Vault is the entity.

**know more about DAICOs.*

FEATURES FOR ATTACK PREVENTION

The membership system prevents 51% attacks with the following measures:

- ◆ Vote capping: No individual can carry a vote weight corresponding to a token share greater than a pre set cap.
- ◆ In case of a coordinated attack by multiple individuals, the platform additionally checks the number of people voting for a refund in addition to total vote share in favour of refund.
- ◆ Health indicator makes the investor aware of the amount of governance participation and apathy levels.

ADDITIONAL FEATURES

- ◆ DEX integration: Vault interface will be integrated with kyber for coins that are listed on Kyber. This is done to encourage participation in governance. More Participation = More Security.
- ◆ One time proposals and step function DAICOs add to flexibility of fund usage.

END-TO-END SERVICE. TOKEN GENERATION TO GOVERNANCE

- ◆ Building a DAIICO is costly, many contracts are written, security audits.
- ◆ User interface standardization is a must, else end users are apathetic.
- ◆ Issuer designing contracts for governance introduces conflict of interests, may result in buried loopholes.
- ◆ Without standardization of DAIICO contract frameworks, investors cannot be sure of the integrity of contracts without performing a tedious audit independently.
- ◆ With vault, investors don't have to worry about going through tons of code to verify, don't need to learn new UI each time.
- ◆ With vault, token issuers don't need to worry about KYC, whitelist, token generation etc.

PRODUCT TWO
STREAM

STREAMLINING OF SECURITY TOKENS

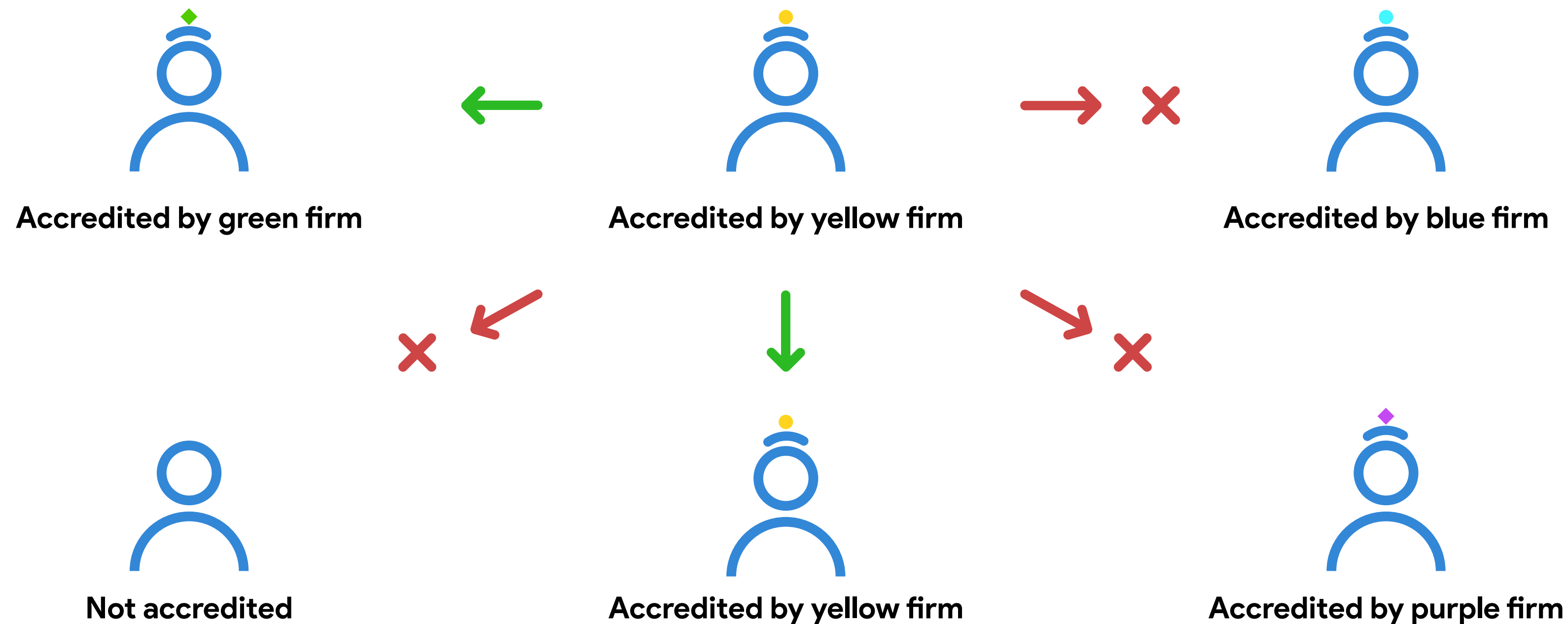
- ◆ Security tokens come with the burden of compliance, the token should not come in possession of individuals who are not accredited investors. Certain companies or security issuers may want to vet the people they want to allow to hold the security, to comply with regulations.
- ◆ The above issues have resulted in several flourishing rent seeker intermediaries who take care of these compliance requirements. They work in time consuming, opaque processes which creates a glut in the market. Investors experience significant reduction in liquidity and increase in compliance costs. This in turn increases cost of capital for the issuer. Doing these things transparently on blockchain adds real value to investors and issuers in the form of liquidity.

ON-CHAIN ACCREDITATION OF INDIVIDUALS

- ◆ Solving the above problems would be possible by creating an entity whose members are accredited investors. Entity would be operated by an organization willing to do the diligence on investors and take the liability, and offer the verification as a service.
- ◆ No identifying information needs to be on the blockchain, just the membership identifier of the electus protocol is enough to streamline tokens.

HOW DOES STRTEAMLINING OF TOKENS WORK?

The issuer of the token that is being transferred here recognises green firm and yellow firm as their accreditation partners and allows their tokens to owned only by addresses that are accredited by them



ACCREDITOR CONTRACT TOKEN

- ◆ It is possible to create tokens under a new EIP that will only be sendable to addresses which are members of a certain entity (or a logical combination of multiple entities) on the blockchain.
- ◆ In addition to restricting to accredited investors, issuers can further choose to restrict their security token to other specific categories of investors(domestic, foreign, etc).
- ◆ This will enable issuers to keep track of their regulatory standing without having to clamp down upon each and every transaction.

ACCREDITATION PLAN WITH SECURITY EXCHANGES

- ◆ When liquidity of securities increases, Exchanges will come into the picture, and will have to integrate such compliance into their withdrawal/trading/deposit practices. The exchange holding address will have to be accredited(and otherwise permissioned by issuer if necessary) by default.
- ◆ The exchange should know which of its customers are accredited and disallow trading accordingly. Since tokens cannot be sent to non accredited(or non permissioned) addresses, the exchange will need minor exception handling on the withdrawal side of security tokens.

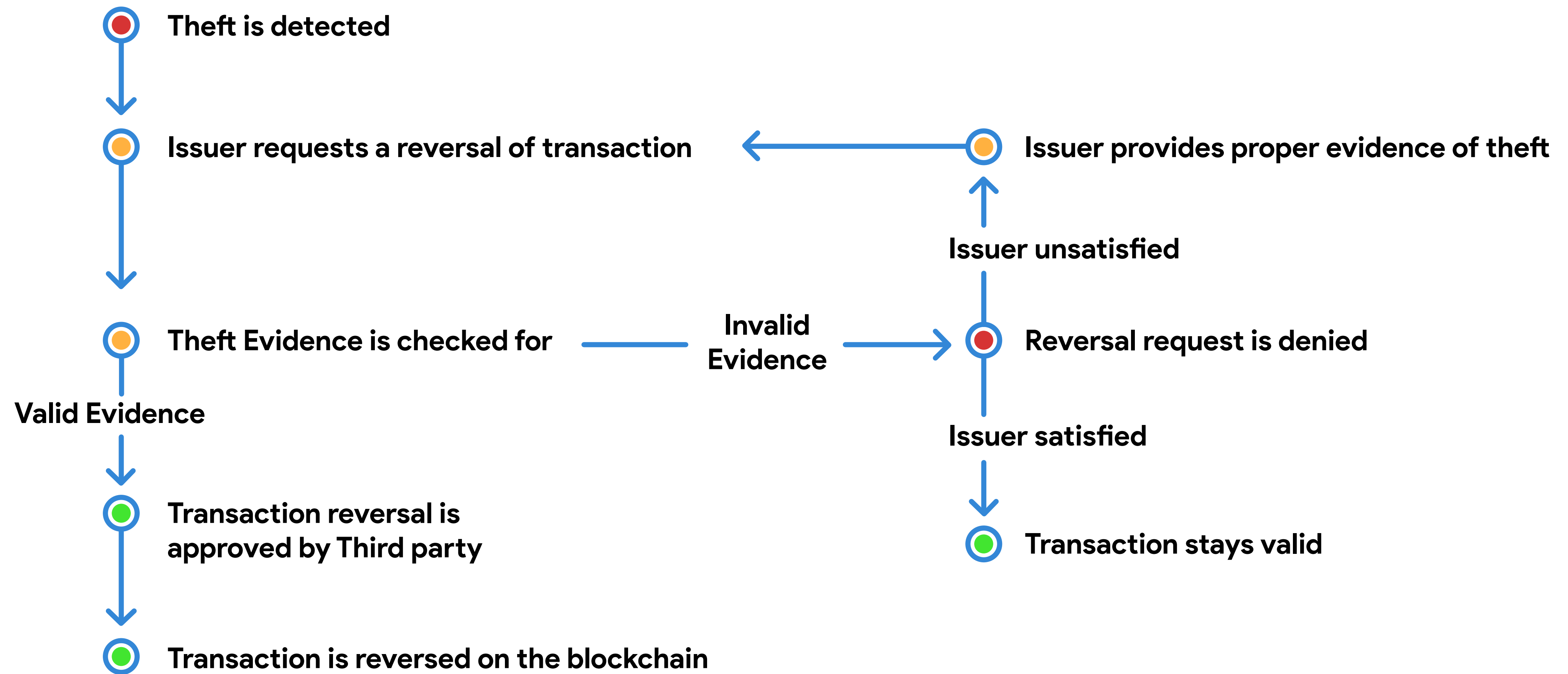
SECURITY TO UTILITY SWITCH

- ◆ During Private sales or Security token offerings, an issuer may take funds from an accredited investor, and later when demonstration of utility is done, may want to swap it out for a utility token(to ensure wider user base or liquidity).
- ◆ This swap can be replaced by coming up with a security token which has a flag that can be switched off, which would convert existing tokens into utilities.
- ◆ The flag can be operated by a third party who takes responsibility for due diligence that utility has indeed been demonstrated, thus removing conflict of interest.
- ◆ The removal of the need to swap results in exchanges, and other liquidity providers not having to go through several hoops to onboard the new token and deprecate the old one.

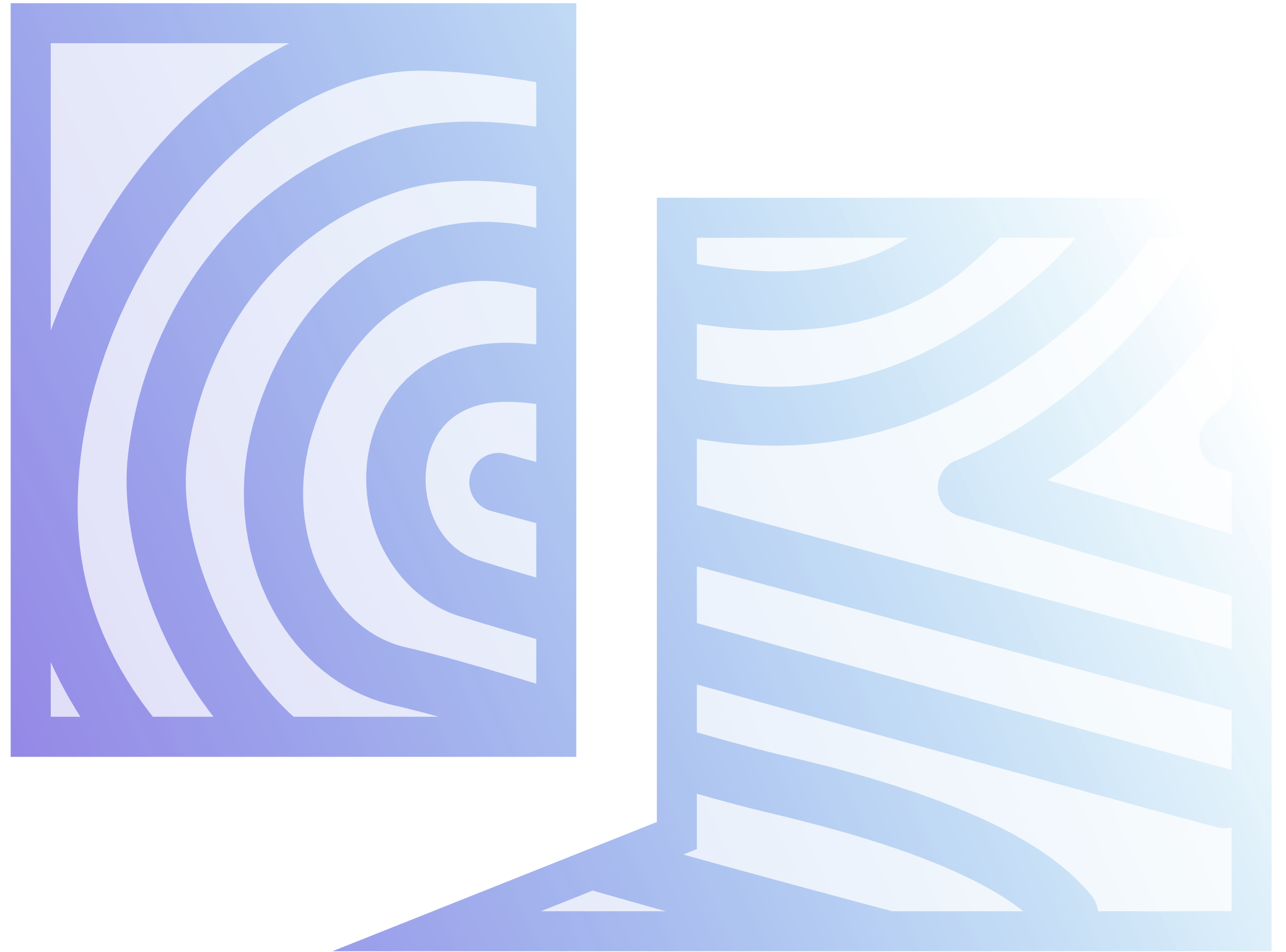
THEFT PREVENTION

- ◆ In the event of theft, a security token can be tracked down to the thief because the accreditor has the data of each permissioned address, and is obliged to reveal the information upon an event of theft. However an additional control is needed. The issuer is legally obliged to return the security to the correct owner. This ability must be baked into the token.
- ◆ But this ability introduces conflict of interest because then the issuer can edit balances without permission. Hence a theft flagging service is needed. An independent body will flag a security token contract with a theft on the blockchain, and also mark the address in which the stolen funds lie. Issuer then allocates the securities from that address to the right person.
- ◆ Contract is designed to allow the issuer to do this only when the theft flag is active. Theft flagging service provider has no incentive to wrongly flag addresses (but has a lot to lose because its actions are publicly visible), because they cannot move funds, and issuer cannot move funds without the theft flag being active. Conflict of interest is gone.

THEFT PREVENTION FLOWCHART



PRODUCT THREE
POLIS



FACILITATING ANY COMMUNITY-FOUNDED ONCHAIN GROUP

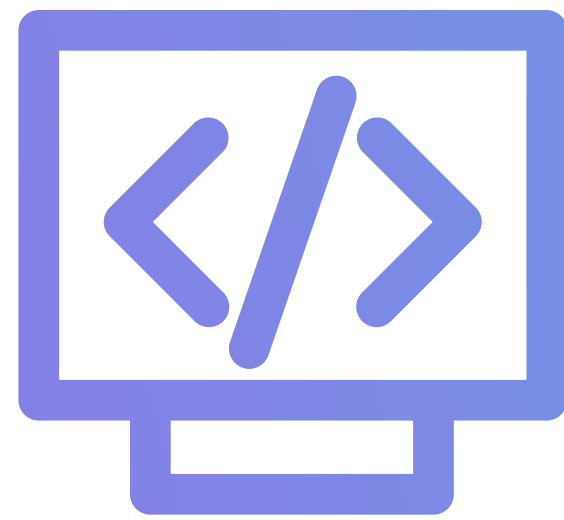
- ◆ Polis will enable reliable direct democracy powered by blockchain. Software which can be used for deployment of governance systems for communities. Users can access all compatible governance systems through the same user interface to take part in consensus. The entity is populated and maintained by an admin, who has no backdoor control over the votes, and cannot delete polls that go against their interest.
- ◆ All admin activity is transparent and immutable on blockchain. So the admin is always answerable. The system enables members of a community/organization to directly contribute to consensus without being subject to censorship, manipulation and spam.

DIFFERENT KINDS OF POLLS

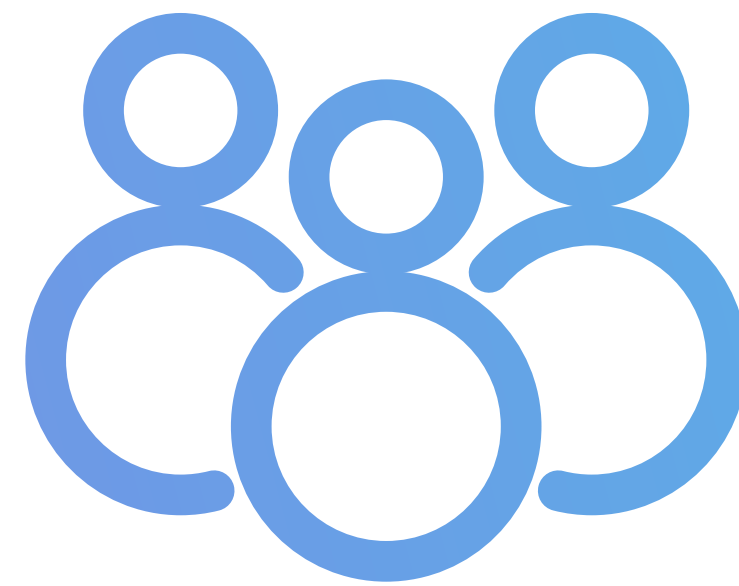
- ◆ One person-One vote for standard issues
- ◆ Delegated democracy for niche areas with specialization
- ◆ Karma based voting for reputation/trust based categories
- ◆ Token balance based voting for matters that require skin in the game
- ◆ Anyone can deploy polls that read from certain entities or combination of entities

DIFFERENT GOVERNANCE/INHERITANCE STRUCTURES

A governance system would be comprised of several entities representing committees, councils and so on. Power relationships can be established either at the blockchain layer or simply at the database layer after reading the consensus from blockchain. This results in flexibility in the kind of governance that can be made possible.



DEV COMMUNITIES



USERBASE COMMUNITIES



FAN CLUBS

OTHER POTENTIAL USE CASES



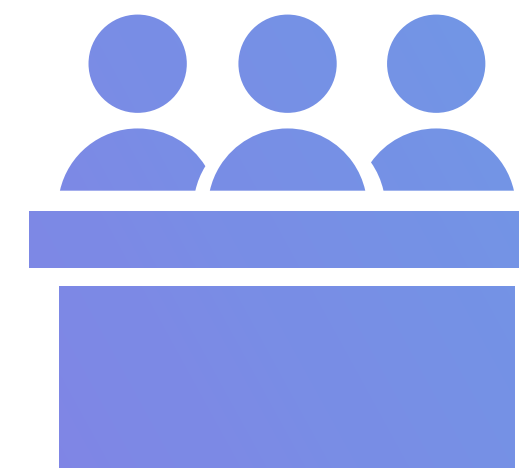
ANTI-PIRACY



ID/PASSPORT/VISA ISSUANCE



CORPORATIONS



*EQUITY STYLE BOARD
OF INVESTORS*



*EVM TRAILS FOR
ELECTIONS*



GOVERNANCE

OF THE PROTOCOL

APEX



WHY GOVERN THE PROTOCOL ITSELF?

As the number of users increases, different stakeholders will prefer different functionalities on the protocol. A system is needed to govern the protocol reliably.

GOVERNANCE STRUCTURE

Electus network will be an entity with a democratically elected admin. Admin will be in charge the entry of new members. Members will themselves be entities who have their own members. Votes are proportional to amount of stake in the system, ie. Electus tokens.

PLATFORM FOR MANAGING PROTOCOL GOVERNANCE

Apex will be the application layer with which stakeholders will manage their governance activities. These activities include voting, changing votes, staking coins and delegating these stakes. Membership requests to the Electus network can be made from the same application.

USE CASE FOR TOKENS

- ◆ Electus tokens are locked up for governance, and locking more tokens gives the member more power in the system.
- ◆ Votes are proportional not only to amount of tokens but also to lock timing, to prevent mass buys and dumps before major decisions.
- ◆ Lock timing can be extended, not reduced, reduction of the lock timing is violation of the initial commitment.

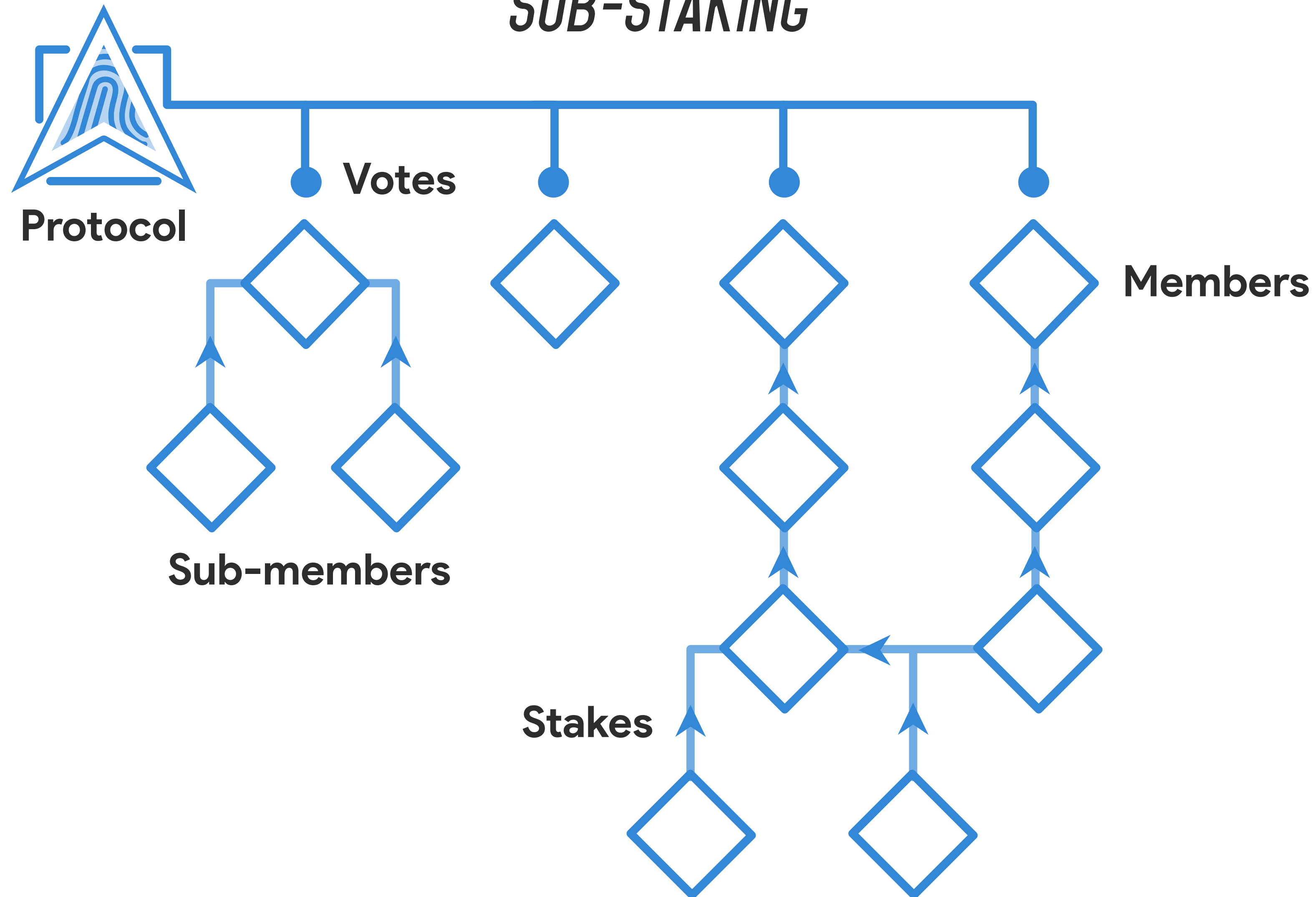


UNDERSTANDING SUB-STAKING

- ◆ Tokens can be staked by individuals who belong to entities that govern the protocol, ie. Members of members and so on.
- ◆ When such individuals stake, their stake is delegated to an entity to which they belong and the entity gains more power.
- ◆ If such a party happens to be member of multiple entities who govern the Electus network, they have to choose the parent in the tree who gets more vote weightage.
- ◆ In return, the child gets internal governance incentives from the parent who received their stake.



SUB-STAKING



TEAM



PARTHA BHATTACHARYA

CEO, Product Lead,
Business Development
Ex-Goldman Sachs
IIT Bombay



CHAITANYA POTTI

CTO, Smart Contract Engineer,
Full Stack Developer
Ex-Credit Suisse
IIT Bombay



SOMESH YADAV

Design Lead, UX/UI Architect
Ex-Leo Burnett
IIT Bombay



ROHAN RATHOD

Backend Development,
Operations
IIT Bombay



AAYUSH GUPTA

Frontend Lead Engineer
Ex-Shaadi.com
IIT Bombay