EdenDAO: A political formalist's decentralized government design

Shogo Ochiai (shogo.ochiai@protonmail.com)

Abstract. Democracy is a state machine, hence you can formalize it. That state machine has the safety property and liveness property for the soundness of the political deliberation. The soundness of deliberation would be defined by the safety and liveness of several public administrations. Given we implement public administrations as DAOs with vested budget, corrupted administration can be dismissed by signatures of people. You see? It is the only possible form of incorruptible government. You'll get "just right" regulations. That "just right regulation" Legos are enable efficient, sustainable, and human security preserving society. This is a DAO framework and members are not limited to any kind of ideology. You can make your country and autonomy on it. Have fun to play yours real-world SimCity :)

1. Introduction

Democracy on the Internet has come to rely almost exclusively on politicians serving as trusted third parties to process legislations. While the system works well enough for most economically bullish seasons, it still suffers from the inherent weaknesses of the trust based model. This paper illustrates the spec of peer-to-peer e-government system which won't be corrupted and even won't broken in the WW-III. Using this protocol advantages early-adopting municipalities and nation-states.

2. Political Formalism

Given a democratic governance model, we define a formal propositions of the soundness of deliberation. We assume if deliberations of a governance are nice, then resource allocation and human rights preservation of the autonomy is always nice. As a side note, we call such attitude as the "political formalism".

2.1. EdenDAO's adversary Model

The goal is to guarantee that democracy is not irreversibly destroyed (having liveness) for all adversaries. It also aims to design the system in such a way that the cost of a weak adversary being able to exploit a security hole and behave like a medium adversary is high. 1.

1. strong adversary:

Able to attack 51 percent of the blockchain nodes for more than 3 days or supply more than 3 years equivalent (billion dollars) of bribes to the police.

2. medium adversary:

Can identify and blackmail a person's whereabouts using only one's name.

3. weak adversary:

Threats can be carried out based on publicly available location information.

2.2. Primitive states and rationale

isProofOfPersonhoodUnsafe

A state where the proof of personhood algorithm is not working well.

isProofOfPersonhoodLive

A state where the proof of personhood algorithm can back to normal in the end.

hasEnoughAnonymity

A state where the people have their own anonymity infrastructure to avoid surveillance or coercion under the heavy adversarial administrations.

hasNoMoney

A state where the person in charge is vulnerable on one's personal financial situation and can be affected by adversarial bribing offers.

assumesHumanRightsImportant

A state where the person in charge of the administration expresses the good attitude for the Universal Declaration of Human Rights

hasItsOwnDetectivesAndWorkers

A state where the adversary has its own PublicKey-PhysicalAddress dictionary (e.g., Google)

isLocationUndisclosed

A state where any responsible entities are accepted to disclose their PublicKey-PhysicalAddress dictionary to the adversary.

isPhysicallyIdentified(Alice)

A state where the physical address of Alice is exposed as a public information.

isInSamePlace(Alice, Bob)

A state where Alice and Bob is in the same place.

is3dReorgSafe

A state where no one cannot roll back the blockchain that EdenDAO is relying on.

isPerpetualPoliceBribingSafe

A state where the police is resilient against ever-lasting bribing offering.

isCommunityBasedPolicing

A state where the community has its own public safety program by their own effort.

isMonopolized

A state where subjects are occupied by malicious entities.

isLargestCorporationNotTooBig

A state where there are no too large corporations in the market.

zkpUnsafe

A state where the masquerade circuit which is made of zk-SNARKs or that cryptography itself are unsafe.

CheckerSubDAO An optional administration which checks the validity of moving-in and moving-out of the autonomy system on behalf of peer-to-peer-based direct check. May not work under extreme scenario.

2.3. Common Utility Predicates

By the composability of primitives, we describe useful predicates to deduct further formal political logics.

$$\begin{aligned} &isDismissible(subject) := \\ &\quad noStrongAdversary \land isKeySellingLive \land hasMajorityInformedCitizenry \end{aligned} \tag{1}$$

$$hasMajorityInformedCitizenry := isMediaLive \lor isEducationLive \tag{2}$$

$$\begin{aligned} &noStrongAdversary := \\ &\quad is3dReorgSafe \\ &\quad \land (isPermanentPoliceBribingSafe \lor isCommunityBasedPolicing) \\ &\quad \land (isPrivateMilitaryRestricted \lor isLargestCorporationNotTooBig) \end{aligned} \tag{3}$$

$$isKeySellingLive := isJurisdictionLive \tag{4}$$

$$isFragile(subject) := (hasNoMoney(subject) \lor assumesHumanRightsImportant(subject)) \tag{5}$$

$$isCorrupted(subject) := isFragile(subject) \land isJurisdictionUnsafe() \tag{6}$$

$$\begin{aligned} &isCoercedByWeakAdversary(subject) := \\ &\quad isPhysicallyIdentified(subject) \land (adversaryPower > policePower) \end{aligned} \tag{7}$$

$$
\begin{aligned}
&isCoercedByMediumAdversary(subject) := \\
&\quad isCoercedByWeakAdversary \\
&\quad \wedge (\\
&\quad\quad \neg isLocationUndisclosed(subject) \\
&\quad\quad \vee (isLocationUndisclosed(subject) \wedge canWeakAdversaryBeMediumAdversary) \\
&\quad)
\end{aligned}
\tag{8}
$$

$$
\begin{aligned}
&canWeakAdversaryBeMediumAdversary := \\
&\quad hasItsOwnDetectivesAndWorkers \wedge \neg hasNoMoney \wedge \neg assumesHumanRightsImportant
\end{aligned}
\tag{9}
$$

2.4. Safety Proposition of each public administrations

If a subset is unsafe, it means that the administration can exert pressure on the outcome of the deliberation.

$$
\begin{aligned}
&isFacilitatorsUnsafe := \\
&\quad (isRandomOracleUnsafe \wedge isCorrupted(self)) \\
&\quad \vee isCoercedByMediumAdversary(self)
\end{aligned}
\tag{10}
$$

$$
\begin{aligned}
&isProfessionalsUnsafe := \\
&\quad (isRandomOracleUnsafe \wedge isCorrupted(self)) \\
&\quad \vee isCoercedByMediumAdversary(self)
\end{aligned}
\tag{11}
$$

$$
\begin{aligned}
&isJurisdictionUnsafe := \\
&\quad (isRandomOracleUnsafe \wedge isFragile(self)) \\
&\quad \vee isCoercedByMediumAdversary(self)
\end{aligned}
\tag{12}
$$

$$
isCitizenRevisionUnsafe := isDocumentVerifierUnsafe \wedge isResidenceCheckerUnsafe \tag{13}
$$

$$
\begin{aligned}
&isDocumentVerifierUnsafe := \\
&\quad (isCheckerSubDAOUnsafe \vee isCitizenCheckUnsafe) \\
&\quad \wedge isProofOfPersonhoodUnsafe
\end{aligned}
\tag{14}
$$

$$
\begin{aligned}
&isResidenceCheckerUnsafe := \\
&\quad isCheckerSubDAOUnsafe \vee isCitizenCheckUnsafe \vee isJurisdictionUnsafe
\end{aligned}
\tag{15}
$$

$$
\begin{aligned}
&isCheckerSubDAOUnsafe := \\
&\quad isPoliceUnsafe \\
&\quad \vee (\neg isInSamePlace(Police, CheckerSubDAO) \wedge isCoercedByWeakAdversary)
\end{aligned}
\tag{16}
$$

$$
isCitizenCheckUnsafe := isDeliberationUnsafe \tag{17}
$$

$$
isPoliceUnsafe := \neg noStrongAdversary \tag{18}
$$

$$
isEducationUnsafe := isCorrupted(self) \vee isCoercedByMediumAdversary(self) \tag{19}
$$

$$
isMediaUnsafe := isCorrupted(self) \vee isCoercedByMediumAdversary(self) \tag{20}
$$

$$
isSurveillanceUnsafe() := isCorrupted(self) \vee isCoercedByMediumAdversary(self) \tag{21}
$$

$$
isMasqueradeUnsafe := isEducationUnsafe \wedge zkpUnsafe \tag{22}
$$

2.5. Liveness Proposition of public administrations

When a subset is live, it means that the administration is able to recover from a situation where it is pressured by the outcome of the deliberation to a state where it behaves in a way that contributes to the fairness of the deliberation.

$$\begin{aligned} &isPoliceLive := \\ &\quad (isDismissible(self) \land noStrongAdversary \land hasEnoughAnonymity) \\ &\quad \lor (isDismissible(self) \land \neg isCoercedByMediumAdversary(self)) \\ &\quad \lor isJurisdictionLive \end{aligned} \tag{23}$$

$$\begin{aligned} &isFacilitatorsLive := \\ &\quad (isPoliceLive \lor isJurisdictionLive) \land hasEnoughAnonymity \end{aligned} \tag{24}$$

$$\begin{aligned} &isProfessionalsLive := \\ &\quad (isPoliceLive \lor isJurisdictionLive) \land hasEnoughAnonymity \end{aligned} \tag{25}$$

$$isJurisdictionLive := isDismissible(self) \land isPoliceLive \tag{26}$$

$$isCitizenRevisionLive := isDeliberationLive \land isProofOfPersonhoodLive \land isJurisdictionLive \tag{27}$$

$$\begin{aligned} &isEducationLive := \\ &\quad (isDismissible(self) \land noStrongAdversary) \\ &\quad \lor isMonopolized \lor isPoliceLive \lor isJurisdictionLive \end{aligned} \tag{28}$$

$$\begin{aligned} &isMediaLive := \\ &\quad isSurveillanceLive \\ &\quad \land (\\ &\quad\quad (isDismissible(self) \land noStrongAdversary) \\ &\quad\quad \lor isMonopolized \\ &\quad\quad \lor isPoliceLive \\ &\quad\quad \lor isJurisdictionLive \\ &\quad) \end{aligned} \tag{29}$$

$$\begin{aligned} &isSurveillanceLive := \\ &\quad (isDismissible(self) \land noStrongAdversary \land hasEnoughAnonymity) \\ &\quad \lor isPoliceLive \lor isJurisdictionLive \end{aligned} \tag{30}$$

$$isMasqueradeLive := isEducationLive \tag{31}$$

2.6. Deliberation Predicates

The fact that deliberation is unsafe means that any entity can control the outcome of deliberation to some extent.

$$\begin{aligned} &isDeliberationUnsafe := \\ &\quad isFacilitatorsUnsafe \lor isJurisdictionUnsafe \lor isCitizenRevisionUnsafe \\ &\quad \lor isEducationUnsafe \lor isMediaUnsafe \lor isSurveillanceUnsafe \lor isMasqueradeUnsafe \end{aligned} \tag{32}$$

$$isDeliberationSafe := \neg isDeliberationUnsafe \tag{33}$$

When a deliberation is live, it has the power to return from a deliberative environment under the pressure of a particular actor to a fair deliberation without pressure.

$$\begin{aligned} &isDeliberationLive := \\ &\quad isFacilitatorsLive \land isProfessionalsLive \land isJurisdictionLive \\ &\quad \land isCitizenRevisionLive \land isEducationLive \land isMediaLive \land isSurveillanceLive \end{aligned} \tag{34}$$

2.7. Wrapping-up

Now, democracy and deliberation are semi-formalized. But due to the nature of nations, real governance is not ideal. The governance system has "path dependency" of what has been built upon it and not always optimal.

Hence we had to formalize and analyse where is the weakest vector of a given governance system without bias of that path dependency.

In this political formalists' view, almost all countries are vulnerable in this point of view and so let's see what kind of country can be secure against adversary model above.

And now you can point out and make diagnosis where one should make sure the liveness of, and what's the suitable policy to make deliberation, human rights, and Pareto efficiency nice.

For example, when a government is not teaching how to exercise their own democratic rights and its history, its education is not safe. And if they can't change their education for a long time due to corruption, it's not live. Note that many countries are in such situation but it's not normal. You have to change that. Furthermore, you can see isMediaUnsafe and isFacilitatorsUnsafe when there is mobocracy (not well deliberated democracy). You have to fix them as well. To fix it, you need to make them "live" and so see the liveness propositions above.

For any scenario, you can build up a cool analysis and diagnosis or what you have to do. Think about abduction and corruption of national ID screening (= citizen revision) administration, judges, facilitators, experts, and council members. Resale of secret key as well may happen. Try looking at political news in the real world and train yourself to get accustomed with these logics.

But you know, such debugging of public administrations in the parliamentary indirect democracy system is very tough. Nothing much changes soon. You can analyse what's wrong but you would leave it because you can't move people. So, legislation have to be more easier and opened to everyone. Of course, with enough DoS-mitigation.

Suppose we have such assumption and belief, let's see what kind of governance framework is useful for such scenario.

3. People, SubDAO, and GovDAO

We describe the very basic actors of EdenDAO-based municipalities and nation-states in this section.

3.1. People

The initial members register themselves to the smart contract. The registration is peer-acknowledgement of the rationale of why is that person is appropriate to be a member (e.g., Immigration Certificate, Move Out Certificate, Newborn Certificate). Those initial members do the "member revision proposal (MRP)" and its deliberation, and so population is to be increased.

3.2. SubDAO

The SubDAO is a Ethereum-ish naming of a public administration. SubDAO works for public welfare, and they are created and assigned by the people. SubDAO's budget is vested on the Ethereum and so they can't steal it at once. If a SubDAO does a malicious behavior, people can hold a veto proposal and can slash their rest of vested budget. And so they don't have any incentive to be corrupted. When they need more budget, they propose improvement plan by themselves with the help of volunteer people for planning.

3.3. GovDAO

The GovDAO is a Ethereum-ish naming of a municipality government and a national government. It is to be categorised in the direct democracy or sortition. Please forget about parliamentary indirect democracy and politicians. This GovDAO holds many SubDAOs, tenure workers, treasury, proposals, and litigations.

3.4. ComDAO

We can use the GovDAO for the community that is being maintained by the peer-to-peer deterrence of tax collection (e.g., PTA, House Owners Association, Industrial Working Group, Global Union for Economic Externality, Religiorous Working Group, etc.) We call such usage of GovDAO as "ComDAO" to distinguish both of them. The GovDAO and the ComDAO are basically the same infrastrucutres, but the most notable difference for the ComDAO is the absence of the police and the tax collector. Additional technical difference is the citizen revision. When you want to add a member to the GovDAO, you do the move-out certificate check or something thorough due-deligence process. But the ComDAO only uses SNS-based account posession check. The SNS (or any other criteria of participation) shall be decided by the deterrence property of each ComDAO.

3.5. Attacks and griefings

3.5.1. Denial of Service

It is possible to submit a lot of moving-in requests.

We learned from Idena blockchain. We use a local and minimal version of Proof-of-Personhood (PoP) Sybil control mechanism. It requires us to register some Flippers from citizen to create the Turing-complete quizzes. We also require some Examiners to execute PoP tests. This throttles possible headcount of "MRP (Member Revision Proposal)" deliberation.

Also, we can make a dedicated administration SubDAO for that MRP acknowledgement process. Only when that "MoveInSubDAO" does some malicious behavior, we slash its vested budget and replace that SubDAO with better ones.

3.5.2. Bad Flip Attack

A flipper is a SubDAO-based quiz-resouce generators. They assemble two stories by pictures to make a common-sense problem.

When a flipper generates non-Turing-complete flips to IPFS storage, Examiner and the people have to veto the Flipper and slash his vested budget.

3.5.3. Bad Examiner

Examiners are tenure job to ask quizzes for moving-in waiting list. What they exactly do is the decryption key revealance. They work for several years. Their allocation is randomly decided by the protocol for each examination sessions, and so if the majority of Examiners are malicious, the Bad Examiner is gonna be a matter. In other words, when education and media are corrupted, deliberation and assignment of tenure people will be bad.

3.5.4. Bad Certificate

The death, newborn, immigration, and moving out of the people could be signed by Ethereum ECDSA and so corresponding signer is to be legally responsible for his intention. This will be a good deterrence against malicious member revision. But the moving in cannot be signed by an eligible member of the GovDAO - that's spontaneous action by the outside resident in the non-GovDAO users. In this case, we have to verify each certificate of moving in that is made by non-GovDAO municipalities or nations. This verification could be done by a SubDAO for moving--out certification verification administration or SubDAO-independent civil deliberations for emergency scenario. The SubDAO could be upgraded by a SubDAO with better verification speed and quality if people make an improvement proposal. This competition makes the certification verification more accurate and high-throughput.

4. Legislation, Deliberation, and Jurisdiction

We describe the details of the legislation process, jurisdiction, and law-friendly stacks.

4.1. Proposal

A registered member of a GovDAO can make a proposal to create an administration, allow budget to them, make a new law, assign a new tenure officer, veto an administration, or update the environmental variables of the GovDAO.

4.2. Leglang

LegLang is a domain-specific language for the proposal and law. First, you can write a problem. Then you can append multiple solutions. Each those solutions have budget commands like a simple programming language, and those also have law section in the natural language. LegLang requires the proposer to decide how are those solutions must be chosen (e.g., majority rule, Borda rule, median voter theorem, quadratic voting).

It would be noteworthy that this LegLang doesn't have to be written in a programming editor. You can wrap all syntax by the mobile app's UI and so you won't be suffered by the technical details.

4.3. Initial Judge

After you submit the LegLang-based proposal to the Ethereum, you are in the initial judge phase. This phase is for DoS mitigation. When a proposal is incoming, quickly several citizens are randomly assembled by the protocol. They are the committee. They glance the problem part of the proposal, and look at who is saying that, then they vote for is it worth discussing more.

4.4. Facilitator Choice

After committee voted for a proposal, the protocol randomly choose a facilitator from the tenure facilitator pool.

4.5. Domain Choice

After the protocol chosed a facilitator, the facilitator choose the domains of the proposal.

4.6. Professional Choice

After the facilitator chosed domains, the protocol randomly choose professionals for each domain.

4.7. Modification Request

Now you are in the deliberation phase. This deliberation phase is a pure discussion among the committee, the proposer, the facilitator, and the professionals. The rest of citizens also can see what is going on here.

The modification request (ModReq) is a intermediate commitment of the status quo of their discussion. Those members above can request a modification against existing latest LegLang-based proposal. A request can be voted by the committee.

4.8. 3-way merge

When two ModReqs are targetting for the same line of the latest LegLang and one ModReq is approved by the committee and when the targetted line has been disappeared, the other ModReq is going to be stalled. In this case, the latter ModReq has to update the base ModReq.

4.9. Final Judge

At the last phase of a legislation, the committee votes for solutions. The way of vote scoring is defined by the proposer, or modified by ModReq. For example, Borda rule is good for getting consensus among multiple different options. Majority judge is big no-no for this case. When multiple gradational options there are, median voter theorem would be better. Some of radical people can use even quadratic voting.

4.10. Law Viewer

The Law Viewer aggregates and make an index of approved proposals. It parses the list of LegLang and renders the readable document of all law in the GovDAO.

4.11. The court

For nation-states usage, the court should preferably be common-law-based three-tiered court system. For municipality usage, you can have your original legal system but you have to be responsible against the rule of upper government.

4.12. The judges

Supreme Judges are assigned by the people in deliberation and they have a tenure track (e.g., 10 years). Those supreme judges are governance committee of the personnel affairs SubDAO of normal judges. Litigations are to be submitted to the GovDAO and get an LitigationID on the chain. That litigation randomly select a judge from judge pool by using on-chain unmanipulatable Random Number Generator (RNG).

4.13. Tenure Job and Random Number Generator

The tenure jobs are trusted jobs. We define facilitators, professionals, examiners, and supreme judeges as tenure jobs. As we can see in the committee selection in the Ethereum2.0, a decent randomness mitigates colluding a trusted job. We use VDF as the source of randomness. Like ChainLink VRF, we can ready a Randao interface which wraps VDF and it's verifier. VDF assume to have at least one honest participant. So it won't make any bottleneck for the entire EdenDAO's security assumption. The participants of this VDF could be chosen by EDN token stakers and the contributors gets decent reward.

5. Coercion and Censorship

5.1. Coercion-resistance in Voting

We take voting security seriously. The security of a voting system is measured simply by fairness. A fair voting system of course correctly counts ballot, but not only that. Coercion and vote-buying undermine the democracy. Coercion is a form of physical threat to achieve a malicious party's political purpose. Vote-buying is a form of bribry to get more ballots for a political purpose. Those two attacks are more effective in the non-surveillance voting (e.g., mobile voting) and voter-identified voting (e.g., non-crypto votings). EdenDAO aims for an identified citizens' mobile voting system and so coercion and vote-buying are inevitable issues. We solve it by a "Masquerade" technique. It is a mixing algorithm of the External Owned Address (EOA) of Ethereum. This mixing is done by a zk-SNARKs-based knowledge proving between an identified eligible address and an anonymous stealth address. Once an eligible identity gets a stealth eligible address, then she can join a deliberation without any political risk.

5.2. Privacy in Taxation

As EdenDAO is a on-chain smart contract, all payments would be transparently readable from anyone on the internet. So we hide the payment information and tax due information through the Tax Collector administration. A Tornado Cash-based anonymous payment levers the algorithm. Rollups are make SNARKs much cheaper and so it's very reasonable to use it.

5.3. Censorship-resistance in Legislation

In Jan 14, 2021, Yoweri Museveni the president of Uganda ordered the internet shutdown during his electional voting day. Ethiopia as well did it in Jul 2020, and Russia experimented it in Dec 2020. All those attack interfare a healthy democracy and blocking-ignorant way of democracy is strongly required. We propose to use EdenDAO with Starlink. EdenDAO is inherently decentralized construction and so no single entity can stop it. Starlink as well is very possibly getting more cheaper and competition in the space internet industry makes it so affordable.

5.4. Fool-proof in physical world

We think human rights and accessibility important. No one has to be omitted from the democracy. Some of you may not good at handling devices and may accidentally lost or be stolen your phone. We anticipate such scenario and offers contract wallet combination of Argent, Authereum, and Argent Guardian. Even if you've lost your phone, the thief have to break the Argent's fingerprint auth and Authereum's password auth. Moreover, the GovDAO can provide an account recovery proposal and so your suffrage could be transferred to a new EOA with the help of your family and friends.

6. Token Economics and HubDAO

We've described how do the GovDAO and SubDAOs work. As this system is inherently secure-by-design, no corruption and manipulation would occur. Now, we show how would this system be rewarding early adopters in reasonable way, and how would the whole system be maintained.

6.1. Community Treasury

60% of tokens will be allocated to this category. The community treasury is a kind of liquidity mining program of a newly participated GovDAO. This incentivises people to use EdenDAO, and accumulates the network effect within its ecosystem such as the common-infrastructures and the developer community. As we present in the fig n (TBD, but basically please imagine $y = e^{-x}$ graph), the community treasury rewards early adopters. This reward is triggered in every 10000 blocks by the claim tx of Keep3r Network's keepers. The amount of reward is to be decided by the treasury size which is denominated in the ETH by using Uniswap TWAP oracle to standardize their own reserve currencies. Additionally, the usage of the Smart Bond (we will describe it in the Chapter 8 "Smart Bond, Smart Fiat, Smart Treasury, and Tax Reduction") has to be discounted from the treasury size calculation to avoid cheating treasury size. If token holders find an untrustworthy GovDAO, they can blacklist it by the HubDAO proposal. This reward is paid by EDN ERC-20 token.

6.2. HubDAO (a.k.a. EdenDAO itself)

The HubDAO is a root DAO of entire EdenDAO ecosystem. It holds many GovDAOs and accumulating fees from each GovDAO's deliberations to the pool contract. This HubDAO is responsible for minting EDN token and governance for protocol amendment is also done in here. As each GovDAO and its SubDAOs are separated governance (democracy), EDN holders can't amend them. What EDN holders can change is the rule of HubDAO itself and template contract of GovDAO. This HubDAO would be implemented in Upgradable EternalStorage pattern and so very flexible to improve.

6.3. Initiators' Treasury

40% of tokens will be allocated to this category. This is the bootstrapping fund for initiation. Brave private investors and core developers will hold it. This fund will be vested for several years and cliffed by using Curve (Uniswap)-ish vester contract. The ERC-20 token contract will have rate information to make time-decay inflation. This rate has to be surely refreshed just before every minting, and the logic of the rate can be the same as Curve Finance's one. And the vester contract factory will make a time-locked vault of the bulk of tokens. As this project will take a decade or more for achieving its goal, the vesting term also could be a decade.

7. ĐVM (Democracy Virtual Machine)

Check out Figure-**??** below.

This diagram shows how the Democracy Virtual Machine works. As we described in the Chapter 3 "Legislation, Deliberation, and Jurisdiction", we uses Leglang as the canonical format for all legislation. In EdenDAO, the legislation can make a SubDAO (Administration), allocate vested budget, and make a privacy preserved tamper-resistant datastore for the SubDAO. For integrating all those components in a developer friendly manner, we introduce DVM as a novel framing methodology of the democracy.

7.1. Hidden Contract

The Hidden Contract looks like a Solidity contract. This is possible because we employ eEVM as the VM on the hidden chain. eEVM is a SGX-embeddable EVM made by Microsoft. As eEVM is based on the Open Enclave SDK and Azure Confidential Computing, we have to make it portable in the future.

7.2. Hidden Chain

This chain is consisted by TEE servers. This construction assumes that no adversaries are in the TEE server to keep the information within the chain secret. Those who wants securer assumption, it'll be nice to have sMPC-based hidden chain. Those nodes generate ECDSA key-pair within the enclave and accept valid hidden txs and encrypt them with other nodes' public keys. Encrypted bytecodes are to be stored in the Ethereum. Each node just trust it as a honest tx. They download those txs and decrypt it by using their own private key. They assemble the same state within the enclave, and process contract logic. The enclave can only hold a few MB and so the hidden contract must be optimized. (Further scaling could be invented afterwards.) When a betrayal discovered, the malicious node's vested budget as a SubDAO will be slashed and remaining nodes switches their encryption keys by omitting the malicious node's public key.

7.3. Privacy Assumptions

The Leglang's command can modify an ACL record and so the hidden state access is securely controlled by the Ethereum's economic-security. A read request from a not permitted SubDAO or citizen will be denied according to the ACL. The ACL syncing oracle is required and the bridge is also a SubDAO. If it failed to update ACL in a timely manner, the bridge SubDAO losts its vested budget. This ACL is to be a state within the Solang contract and so easy to use for the assertion logic. When the TEE server manager tries a side channel attack against the enclave, the encrypted bytecodes and hidden state will be revealed but it costs a tremendous trust of the cloud platform.

7.4. Deployments and Setup

As a initial prototype, we employ an Azure image that has an ECDSA key generation program and an eEVM program. Anyone can verify whether it has a backdoor or not. For the deployment of a hidden contract which is for the public service provision of a SubDAO, the Azure image reads Ethereum state and verify if it is eligible deployer or not.

7.5. Scaling of the Hidden Chain

The hidden chain is made of TEE and so the storage limitation is critical in some scenario. For instant scaling, we can make shards for each pair of the hidden contract and the SubDAO or can make checkpoint to prune logs. But such scaling undermines the composability among various hidden contracts to make a complex administrative collaborations and we want both composability and scaling. At April 9, 2021, the DCsv2 series of Azure Confidential Computing has 168MB of Enclave Page Cache (EPC) memory at most. This would be the maximal state size that a shard can contain and bigger GovDAO will suffer from this limitation due to its massive population. On the other hand, Arm's Cortex-m7 has up to 16MB of TCM (Tightly-Coupled Memory). That's noteworthy that those TEE chips are to be enhanced as time goes on, and the composability of hidden contract will be much expressive. Until then, let's just use it with minimal composability.

8. Calculations and Scalability

Validation of the feasibility of entire EdenDAO's planning is a very important factor. Let's see how this works in the real world.

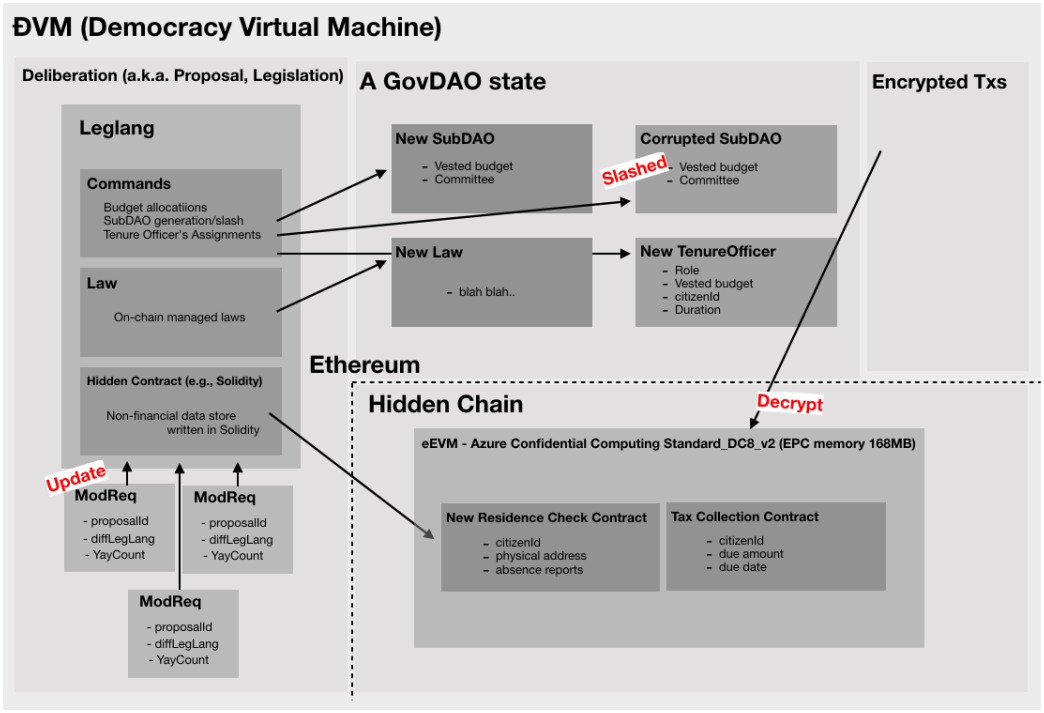

Figure 1: The ĐVM data flow

8.1. Sidechains, Rollups, and Optimism

Municipalities and Nation-states are very huge in budget. For example, Catalonia in Spain has $42B per year of tax income and having such amount of money on the private chain is infeasible. A weak dPoS chain as well won't be stable in this assumption. Only Ethereum's Layer-2 solution works well. For Mar 2021, Optimism is a top-notch Rptimistic Rollup researching company. The pros of Optimism is a full EVM compatibility. Many solidity design pattern is gonna be inherited.

Starkware is also researching zk-Rollup since the day 1 of the STARK scene. StarkNet is their protocol and it could be managed to run EVM on it, but we assume it won't be completely the same VM with the current EVM.

The scalability of Optimism is very high. Comparing TPS is not an accurate metrics here, hence, let's see gas reduction. The Ethereum2.0 Phase 1.5 would be released in near a few years and then calldata cost will be negligible. What only matters is the zk-SNARKs verification cost. As Groth16 or PLONK are succinct algorithm, thsoe won't harm so much computation resource of the aggregator node of Optimism, but we would better carefully look at this point. If the Optimism aggregator is not good at calculating paring, the gas metering of the anonymous payment or mixing can be relatively expensive. So my 2 cents is investing in pairing friendly Optimism node in the future by us. This will lower the burden of each GovDAO and the user experience will be much better.

8.2. Order of proposals and deliberations

We have many default tenure jobs on the GovDAO. According to a simulation of a developer [**?**], for a town with 326 people, if we want 150 approved proposals per year, we would need 15 facilitators, 1 professional, 3 supreme judges, and 3 examiners. For a city with 7,000,000 people, if we want 2000 approved proposals per year, we would need 150 facilitators, 150 professionals, 15 supreme judges, and 100 examiners. 150 approved proposals requires 22 assignment proposals. 2000 approved proposals requires 415 assignment proposals. For making this amount of assignment deliberation feasible, we have to make those assignment proposals easier and quicker. So we have to research how a assignment proposal could be done in a 3 days with enough personality check.

8.3. Member registration throughput

Mumbai, India is a good model city for this matter. Mumbai has 20,000,000 people in the city at 2020. Aproximetry 100,000 people are moving in to the city. As we mentioned in the section 1, we only have to take care of the moving in because only this type of member registration doesn't have any recommendation sign from eligible member of the GovDAO. 100,000 registration per year means 273 people per day. A specialized SubDAO for verifying those 273 certificates of moving-in would work well for that amount. In case the SubDAO is corrupted, people can check that 273 people in the deliberation. It would be a tough job but we can reward them from GovDAO treasury. The EdenDAO's GovDAO can deal with even Mumbai, and so other cities and town are much more easier. For nation-states, "moving-in" doesn't exist but immigration do exist. This is totally the same as current nation-states, just delegate that job to SubDAO.

8.4. TPS of tax payments

The tax collection is consisted of an account mixing phase, a tax due announcing phase, a fund preparation phase, an actual on-chain payment by the stealth address, and the private preimage revealance to the tax collector. This protocol has two SNARK verfications and RUs can scale them up.

The on-app proving would be optimized by a Rust-based parallel prover and PLONK-based faster SNARK algorithm.

8.5. TPS of Masquerade

Masquerade has two SNARK verifications. The first is for mixing of accounts. The second is for reward payment by providing proof of participation.

9. Smart Bond, Smart Fiat, Smart Treasury, and Tax Reduction

EdenDAO offers DeFi-native features for nation-states and municipalities.

9.1. Smart Bond

The Smart Bond is an ERC-20 token. You can issue it by GovDAO's legislation process. This works just like a public bond, but you can use it on DeFi. In other words, no fee goes to financial institution in regard of issuance. Uniswap works as a second market of public bonds, Compound lends DAI by bonds. Option AMM makes options of bonds. Set Protocol makes a risk-parity derivative of several asset-classes. This untapped demand boosts the sales of municipality bonds and national bonds. Using EdenDAO let them outstand a lot.

9.2. Smart Fiat

The Smart Fiat is an ERC-20 token. You can issue it by GovDAO's legislation process. This token is a stablecoin but not backed by underlying assets. It is just a DeFi-native Fiat. This token is very stable without demanding a lot of ETH collateral. It means DeFi gains more various asset-class than ever. Of course a nation or a municipality unnecessarily use the Smart Fiat. They can use DAI or other arbitrary currencies. This Fiat could be restricted by the on-chain rule by the governance against the UpgradabilityProxy contract. In other words, we can harness the MMT-esque hyperinflational nightmare.

9.3. Smart Treasury

The Smart Treasury is a destination of your tax income. What makes is "smart" is of course its DeFi-native property. This treasury is capable of providing idling money to the yield farming protocols. The accrued alpha is automatically accumulated to the Smart Treasury and it compounds your tax payments.

9.4. Tax Reduction

All those DeFi-native feature is not for making administrations fatter. Those are for posing selective pressure to administrations - your tax due is gonna be automatically fewer . This mechanism forcible making government competent.

10. Split and Merger of GovDAOs

Nation-states and municipality could be separated or united. So the GovDAO has to support such split and merger by default.

10.1. Split of GovDAO

When a GovDAO is splitted to two GovDAO, a splitting proposal is to be initiated. This is gonna be border agreement deliberation. And the residents are to be migrated accordingly.

10.2. Merger of GovDAO

When a GovDAO wants to merge with the other GovDAO, merge contract enable importing the population and treasury of the latter GovDAO. It initiates a proposal in the latter GovDAO and requires a deliberation.

10.3. Nest of GovDAO

A municipality belongs to a nation-state. This is a kind of a social consensus. From the nation-state's point of view, the municipality seems to be agreeing to pay tax to the nation and obey to the national law system. From the municipality's point of view, the nation-state is useful as a uppor governance. So if the municipality wants to change the uppor government, they have to secretly find a new upper government or protect themselves. It is noteworthy that if a citizen in a municipality didn't pay tax for a nation-state, the nation still ought to acknowledge a suffrage for her until the municipality explicitly announce that they now belongs to a new upper governance. At the moment, the former nation processes "member revision proposal" to get rid of the suffrage. So, tax payment status is indifferent from one's suffrage.

11. Timelock Meritocracy

WW-III is headachy problem for e-government designers. COVID-19 is also troublesome to handle in the democratic country. We'll show how EdenDAO deal with them.

11.1. The vulnerability of parliamentary democracy.

The parliamentary democracy is entrusting works to politicians. This means, there exist a need for justifying feasibility of constraints on human rights. The human rights are foundation of freedom of speech and suffrage. Entrusting power is a totally trustful manner of governance.

11.2. Timelock Meritocracy

As EdenDAO is an on-chain-native protocol. We can bind a person not by law enforcement but by protocol enforcement. Code is more than law, more like, code is just a code. We'll see how powerful it is. Now, we set some emergency professionals as tenure professional role. They are chosen by people via deliberations. They can get shit done only in the limited time scope (e.g., 2 months). They are powerful trusted people and they might be able to scatter many legal coordinations with in their term, but that risk is limited at most to the timelock duration.

12. Conclusion

Government redefined. No corruption, no one would be abandoned, and competition prunes excess fat from public goods. Early adopters will get rewarded.

References

[1] the fairest democracy, *2020, Shogo Ochiai* https://www.ted.com/talks/the_fairest_democracy

[2] Strong Democracy, *1984, Benjamin R. Barber* https://en.wikipedia.org/wiki/Strong_Democracy