ContinuumDAO White Paper

10th August 2025

Welcome to Continuum

An open public cross-chain network secured by Multi-Party-Computation and run as a public good.

About ContinuumDAO

ContinuumDAO is a community that is collectively building a future in which all blockchains are linked, to enable the integration of decentralized blockchain ledgers for all dApps. We realise that the entirety of finance and other ‘trust’ based networks will transition to web3 in the next few years and that the biggest opportunity for blockchain is to provide DeFi like services for actual businesses, whether that is to raise capital, or allow investment in assets or provide services that it would be impossible to do so using traditional tools. A future open to everyone, not just in the financial centers of the world. To do this though, it is necessary for all blockchains to be able to communicate with each other securely. This is urgent, since it seems likely that the number of chains will only increase. That is the mission of ContinuumDAO.

As the backbone of ContinuumDAO, we have the first public institutional grade Multi-Party-Computation (MPC) node network called the Continuum. This, together with our system of on-chain and cross-chain governance and our commitment to open source code and permissionless architecture, forms a strong and durable framework, creating an open protocol that everyone can help run, and anyone can contribute towards, that is owned by the community. An unstoppable system, just like the internet on which it runs.

Why Does Having Open Public Infrastructure Matter?

A better question is why would anyone who wishes to create a multi-chain dApp rely on an infrastructure that wasn't completely decentralized, or which was owned by a company, knowing that this could disappear at anytime? ContinuumDAO has sophisticated governance controlled smart contracts that do not rely on a 'team' to administer or update them. The MPC nodes that collectively sign cross-chain transactions can be run by anyone and when we have implemented our road map, a dApp will be able to choose whatever MPC node group it wishes to use. The number of MPC groups is unlimited and so the capacity of the cross-chain network can grow as demand increases, effectively in an unlimited way.

Why is the ContinuumDAO Mission Important?

The existing landscape of web3 is confusing for new and even existing users. Continuum will solve one of the biggest pain points - how decentralized applications (dApps) securely communicate between any blockchain that supports a contract based system.

Limitations of Blockchains

Perhaps 4% of the world's population, but only 10% of smaller businesses may have had some (often limited) interaction with blockchains, Whereas some 81% of the world's top 100 public companies are actively using blockchain for applications like supply chain management, payments, and data security, it is usually in a very limited way. Even these use cases are often spread across a proliferating number of blockchains, with limited ability to communicate between them securely.

Individual chains are restricted in their transaction rate due to block limits, increased gas costs and traffic. Those that are more scaleable often lack decentralization (the 'Blockchain Trilema'). The number of chains is exploding, with L2's on Ethereum, Bitcoin and other major chains. It is easier than ever to create a new blockchain. Given that an expanding number of blockchains is inevitable, the issue is still how to provide secure messaging between these chains.

Lack of Open Cross-Chain Fabrics

Existing cross-chain architectures are sometimes ‘black-boxes’, so that no one is aware of who is signing transactions on destination chains. Others are secured by nodes run by a few individuals, often team members. They do not allow anyone to contribute to cross-chain signing. They are not ‘public’ infrastructure. They are almost always run by centralized entities (companies), so that even their continued existence is in serious doubt.

Security Relies on ‘Staking’ Alone

When a cross-chain messaging system relies on node-runners staking on their nodes alone, then the issue, as the volume grows, is that the value of the staking would become low compared to the value of the traffic itself. There is not a good enough incentive to avoid foul play. The cross-chain signing mechanisms need to be inherently secure without relying on staking alone.

The Number of Chains in a Network is not Scaleable

Sometimes (and this includes some of the most popular bridges) the cross-chain signing relies on multi-signature wallets. The issue here is that multiple signatures are costly. It is hard to upgrade every node to include a new chain that they must sign on. This will prevent support for all but a few major chains and limit the scalability of web3 to the general public.

Technical Challenges in Expanding the Cross-Chain Network

Systems secured by zkProofs are difficult to expand. The zkProof is computationally expensive and requires expensive hardware, which can be challenging for most node-runners to implement. Generating a zkProof from an EVM to a non-EVM is difficult (impossible?) to achieve.

Lack of Protocol Level Security

Systems that use zkProofs and relayers of those proofs do not have protocol level security. It is up to the dApp to choose the relayer and they can switch at any time from within their frontend to an insecure or malicious relayer, unbeknown to the users of those dApps.

How is ContinuumDAO Different?

- Our cross-chain network, called the Continuum, is run by a DAO and designed for autonomous operation. All critical operations and financial transactions depend on on-chain voting. There is no central 'team'.
- The cross-chain signatures are generated by MPC, which is well recognised by institutions as being secure. MPC signatures are collectively made by an MPC Group, but the private key is constructed in a way so that no node has knowledge of more than part of it.
- The number of nodes in a Group that collectively sign can be selected when the Group is formed. The higher the number, the more secure, but the slower will be the signatures. ContinuumDAO will soon enable 'pre-signing', to speed up the computation and allow larger MPC Groups.
- An MPC signature is just a single signature and consumes only limited gas on the chains it operates on. This is distinct from multi-signature solutions. This means that MPC based cross-chains signing is cost-effective.
- Any number of blockchains can join the Continuum. There is no limit, since the number of MPC Groups is also unlimited.
- Anyone can run a node in the MPC network. These nodes can combine to form MPC Groups and then governance voting decides which MPC Groups may sign cross-chain signatures.

- Nodes in MPC Groups receive rewards from the protocol for their work, but the amount of rewards is proportional to a Quality Factor, determined by Governance. This incentivizes well run nodes on quality hardware. Having said that, the hardware requirements to run an effective node are not high and anyone could do so using a standard VPS.
- Nodes will monitor each other for malpractice. If any nodes misbehave, then Governance can lock the staked tokens (veCTM) and these cannot be sold or transferred. This is just a supplement to the inherent security that MPC already has.
- Any blockchain with a smart contract system is accessible from the MPC network. ContinuumDAO has already connected some 30 EVM chains on testnet, as well as TON, Stellar Soroban and will soon be able to connect to Solana and NEAR. SUI and other Move based chains are in our road map to integrate.
- An MPC network has protocol level security. It does not rely on any dApp to choose for instance a zkProof relayer. Whichever MPC Group a dApp chooses will have the same high level of inherent security that comes with the MPC algorithm.
- ContinuumDAO's code is open source. This includes the cross-chain messaging system callable from dApps (C3Caller) and then once it has been audited and thoroughly tested, the MPC code itself will also be open sourced.
- Unlike any other MPC based solution, with Continuum, each individual MPC signature can be tracked and monitored with an API. This ensures that users know which MPC Group and nodes within this group actually signed their transactions. It is easy to spot if there is any centralization - one of the biggest risk factors as we have seen with the failure of other protocols.
- When a node runner registers their node, they can optionally identify themselves with email, Telegram and their name. Anyone using Continuum should know who is signing their transactions and should be able to contact them if they wish to, or at least they should know that they cannot, if the dApp is using an anonymous MPC Group, which it is of course their choice to so so.
- Any dApp can permissionlessly use cross-chain services offered by ContinuumDAO. They may wish to work with the DAO to help develop their application, but there is no obligation.
- Any dApp using Continuum's MPC network pays per byte for cross-chain traffic in a simple and unambiguous way. The dApp simply needs to top up their wallet

periodically with either CTM (the native utility token), or a USD stablecoin. They can pass this charge on to their users if they wish to do so. The per-byte fee is set by governance. The funding model is clear.

The Current Situation

ContinuumDAO was formed in August 2023 by a small community. At this time a simple *non-transferable* ERC20 token called CTMDAOVOTE was airdropped to the community to allow voting. The DAO created its Constitution, that can be read here. The DAO also created its Mission and Vision. The formation of and discussion on proposals happens in our Forum and voting on proposals happens on Snapshot here.

We are currently in testnet with its MPC signing code, our cross-chain messaging system, C3Caller and our voting-escrow contract veCTM. Much of our code is currently being audited by QuillAudit. Once we have passed the audit, we will launch mainnet and distribute our token CTM to stakeholders and core contributors to the DAO.

Over the last year, the DAO has also been working on some projects that will use Continuum. This includes Theia, a cross-chain router for ERC20 tokens, AssetX (currently being audited), which is a Real World Asset Tokenization factory and Lawracle, an protocol that will link law firms to web3 ventures, to provide on-chain proofs of important facts, such as ownership of property, provenance of assets and the veracity of statements made by protocols. Theia is owned by ContinuumDAO and both AssetX and Lawracle will give 50% of their tokens to the ContinuumDAO Treasury. This will be the model for the future of the DAO, to increase Continuum's usage and build up the Treasury's reserves.

ContinuumDAO Roadmap

(1) Formation of a company in RAKDAO to provide legal certainty for ContinuumDAO. Estimated incorporation date is in Q3 2025

(2) Audited code for ContinuumDAO's voting-escrow token, veCTM, the cross-chain messaging system, C3Caller and AssetX. Estimated delivery Q3 2025

(3) Decentralization of the MPC architecture to allow many MPC Groups and to permit dApps to select which ones they wish to use. Estimated delivery in Q4 2025

(4) Testing Governance, combining the enhanced on-chain OpenZeppelin Governor contract and veCTM. Conduct tests for Treasury control, Committee elections, cross-chain smart contract control and proxy upgrades. Estimated completion Q3 2025

(5) Our intention is to launch Continuum on mainnet in Q4 2025, after our public testnet and audit. We have not yet decided on which network we will launch though.

(6) TGE Q4 2025. Distribution of veCTM to contributors and airdrop recipients.

(7) Establishment of a DEX trading pool for our token CTM. Possibly we will also launch on one or more CEX platforms.

(8) Extension of the Continuum MPC network to non-EVM chains such as Solana, Soroban, NEAR. This work will continue throughout 2026

(9) Pre-signing of MPC signatures to speed up the network. Though not essential, this is a performance goal that will be carefully implemented in Q1 2026

(10) Audit of MPC code and open-sourcing of it. Estimated time Q3 2026

(11) Lawracle. This multichain protocol for Legal services related to RWAs will be built by ContinuumDAO. We intend to launch it on mainnet by the end of Q1 2026.

(12) Business development will be a focus from just before mainnet and thereafter. We will work with any protocol that wishes to build using Continuum. We will actively help build these dApps if it make sense for us and the protocol team to do so. Such decisions will always be subject to DAO voting.

Governance

Why Have we Built a DAO?

The adoption of a DAO for Continuum is not just a governance choice; it is a strategic necessity to unlock the full potential of multi-chain dApps. By leveraging the DAO model, we ensure that the services remain decentralized and transparent.

Here's why a DAO is the ideal structure to control permissionless multi-chain services

Decentralized Trust

Real world usage of blockchains requires a high level of trust to attract traditional investors and custodians. ContinuumDAO enhance this trust by distributing governance power among stakeholders, preventing any single entity from exercising unilateral control over critical decisions. Furthermore, DAO-driven decision-making ensures the security and resilience of the Continuum, the underlying MPC network, which serves as the cornerstone of ContinuumDAO and its innovative derivative products.

Efficient and Transparent Asset Governance

Cross-chain services require ongoing governance to manage risks, evaluate asset performance, and adapt to regulatory changes. On-chain governance provides a transparent framework where all decisions are recorded and auditable on the blockchain.

Resilience Against Centralized Failures

By decentralized governance and treasury management, ContinuumDAO minimises single points of failure that could jeopardize the service, which will reduce the risks associated with centralized mismanagement and should effectively guarantee the continuation of the service, so long as there are node runners willing to run nodes and dApps wishing to use it.

Governance Model

ContinuumDAO adheres to a Constitution that is here . The Constitution also states how these rules may be changed by the DAO.

All business of the DAO is kept in our Forum here, especially the formation of new ideas and development of new proposals. Only proposals that conform to the Mission and Vision of the DAO, as laid out in the Constitution are eligible.

Governance roles

There are three governance roles: Committee, Contributor, and Citizen.

- **Committee**
    - The ContinuumDAO committee are currently responsible for signing transactions in multi-sig wallets that will perform asset transfers as directed by DAO voting. The Committee also have administrative signing rights to all administrative smart contract functions, enabling re-deployment, withdrawing or adding funds to contracts, as well as other administrative specific contract functions. All signing of contract functions will initially be via multi-sig wallets. Ultimately, the use of multi-sig wallets for asset transfers and signing administrative functions in smart contracts will be replaced with direct on-chain governance through voting, using an Execute function in a contract controlled by a method such as the OpenZeppelin Governor suite of smart contracts in the veCTM token.
- **Contributors**

- To achieve the ContinuumDAO Mission and Vision, we need a sophisticated DAO structure that can gather talented individuals from diverse backgrounds, respond quickly, and provide professional experience to the DAO. Additionally, we require a fully decentralized node network to ensure service stability.
- ContinuumDAO has a group of full-time people, or Core Contributors group. They are responsible for operating the frontend servers, official accounts, and other related tasks, such as paying bills from assets transferred to hot wallets from the Treasury. The performance of the contributors will be reported each year in the DAO to evaluate.
- There are four Guilds: Research, Business development, Marketing and a Developer's Guild. The guild leader will develop each guild that will support the activities of new projects joining the Continuum.

- **Citizens**
  - Will have the right to join the governance process, which includes proposing, voting, and making contributions. A Citizen can raise a proposal, so long as it conforms to the DAOs Mission and Vision and they control a threshold amount of veCTM power, either in their own wallet, or delegated by other voters to their wallet. The instructions for creating a proposal are detailed here

DAO incentive system

The ContinuumDAO may utilise tokens and the welfare system to boost the performance of all DAO members.

- Full-time contributors and guild leaders will receive monthly payment to attract and maintain dedicated workers, as in any traditional business.
- Node runners will receive rewards based on their performance and other requirements.
- Guild members will receive payment based on contributed work and the outcome of the guild missions.

The ContinuumDAO Token

Vested Token Model

ContinuumDAO has implemented its token model on testnet (Arbitrum Sepolia for now)

Any holder of ContinuumDAO's token (called CTM) can stake them into an NFT called veCTM (see the code on github). The staking is live at https://staking.continuumdao.org . There will be a buy pressure for CTM, since it is used as a payment token by dApps for cross-chain services. This will counteract any sell pressure from node-runners who are paid in CTM and DEX liquidity providers selling tokens. This increased volume should benefit LP providers and attract DEXes and CEXes to list CTM.

The veCTM token is used for governance. It allows on-chain governance using OpenZeppelin's Governor contract, with extensions added by ContinuumDAO to allow multiple choice, multiple selection and weighted voting. Using our cross-chain messaging system, C3Caller, the governance becomes cross-chain, as well as on-chain. This is the system that ContinuumDAO will use to maintain its smart contracts on every chain.

Any multi-chain dApp deployed using C3Caller can also natively utilise this cross-on-chain governance, so that it can be used to maintain all of the admin functions, so that these can be controlled by a protocol DAO, with no central control.

The veCTM token is also used to stake on MPC nodes, adding an extra security measure to the inherently secure MPC algorithm. Only the DAO can un-stake these veCTMs, allowing a bad actor's veCTM to remain locked forever. Node runners will receive payment for their service in CTM, with the remuneration rate determined by DAO governance.

As well as being used for governance (via veCTM) and distribution of payments to node runners, CTM will also be used as a payment option for all services in cross-chain messaging system, C3Caller.

The vested NFT token (veCTM) can be split into two NFT's, so holders can sell part of their holding, or they can be added together. It will be possible to liquidate a veCTM with the holder receiving 50% of their CTM tokens for a 4 year lock, increasing linearly to 100% for a zero time lock. The balance of the CTM tokens will be returned to the DAO treasury. The ability to split, merge and liquidate veCTM solves a long standing problem in DeFi, whereby stakers felt trapped. The new system provides a balance between only allowing staked CTM (as veCTM) to vote, so that those with the medium term interest of the protocol alone determine its actions, but still allowing an escape route, albeit with penalties. Since veCTM adheres to the ERC721 interface, it can also be sold on any NFT marketplace.

The MPC Network

ContinuumDAO's MPC network is live and running and can be viewed at https://dashboard.continuumdao.org

ContinuumDAO is the first **public** MPC network, which means that anyone can run an MPC node and potentially contribute to supporting cross-chain messaging, or indeed other future MPC applications, such as MPC wallets. The MPC system we use and why MPC is a superior system for collective signing is described here . There is no limit to the number of nodes that can contribute to the network, or the amount of web3 traffic that could be accommodated. Individual nodes can be added to an MPC Group permissionlessly. The number of nodes in the group can be decided based on the degree of security required vs the speed of signing. Typically 3-7 nodes would be used. A Threshold number of these nodes are required to sign and this threshold can also be decided permissionlessly. The end result is an MPC node group which has a Public Key. The address derived from this key can be used by a messaging system (in our case C3Caller), or an MPC wallet, or for diverse other applications.

Public MPC Nodes

The instructions for running a node are in our documentation . After someone has created a node, they can attach a veCTM to it. As part of the attachment process, they

can optionally identify themselves, with this information being stored in our node smart contract and publicly visible.

Staking on MPC nodes is live on testnet and can be managed at https://staking.continuumdao.org . The attachment of veCTM is a further security measure beyond the inherent security of MPC, since whereas they can attach the veCTM themselves, only a DAO vote can detach their veCTM and whilst it is attached, the veCTM cannot be liquidated or transferred to another address. A 'bad actor' running an MPC node will have their veCTM permanently locked. Anyone contributing to the MPC network will receive rewards from the DAO in CTM. The reward system that we have implemented (accessible from the staking panel) allows the DAO to score individual nodes out of 10 depending on how well they are performing (up time, speed). The reward is multiplied by the score. In this way we incentivize high quality nodes. The staking system is live on testnet.

Anyone can create an MPC node group, but this does not mean that it is automatically used for signing. As an example, ContinuumDAO's cross-chain messaging system C3Caller can choose which MPC groups to use and the public address of the MPC Group has to be added by a governance vote. Naturally the DAO will choose MPC groups which have the highest veCTM stake and also where the nodes have provided maximum information about who is running them, including potentially KYC. It makes sense though that a decentralized application would have a few MPC groups between which they could switch, so that a problem with any one of them would not compromise the entire dApp. It is entirely up to a dApp to decide which MPC groups they want to use. They could for instance use MPC groups formed from their own community.

C3Caller Cross-chain Message Passing

C3Caller (see the code on github) is the system added to each blockchain that can interface with the MPC network to allow a dApp on one chain to sign a contract function on another chain. Full details describing it and about how to use it are provided in our docs . Any dApp can permissionlessly register the addresses of their main entry contracts on each chain using the web interface at https://c3caller.ContinuumDAO.org . The admin can top up their account with CTM or a

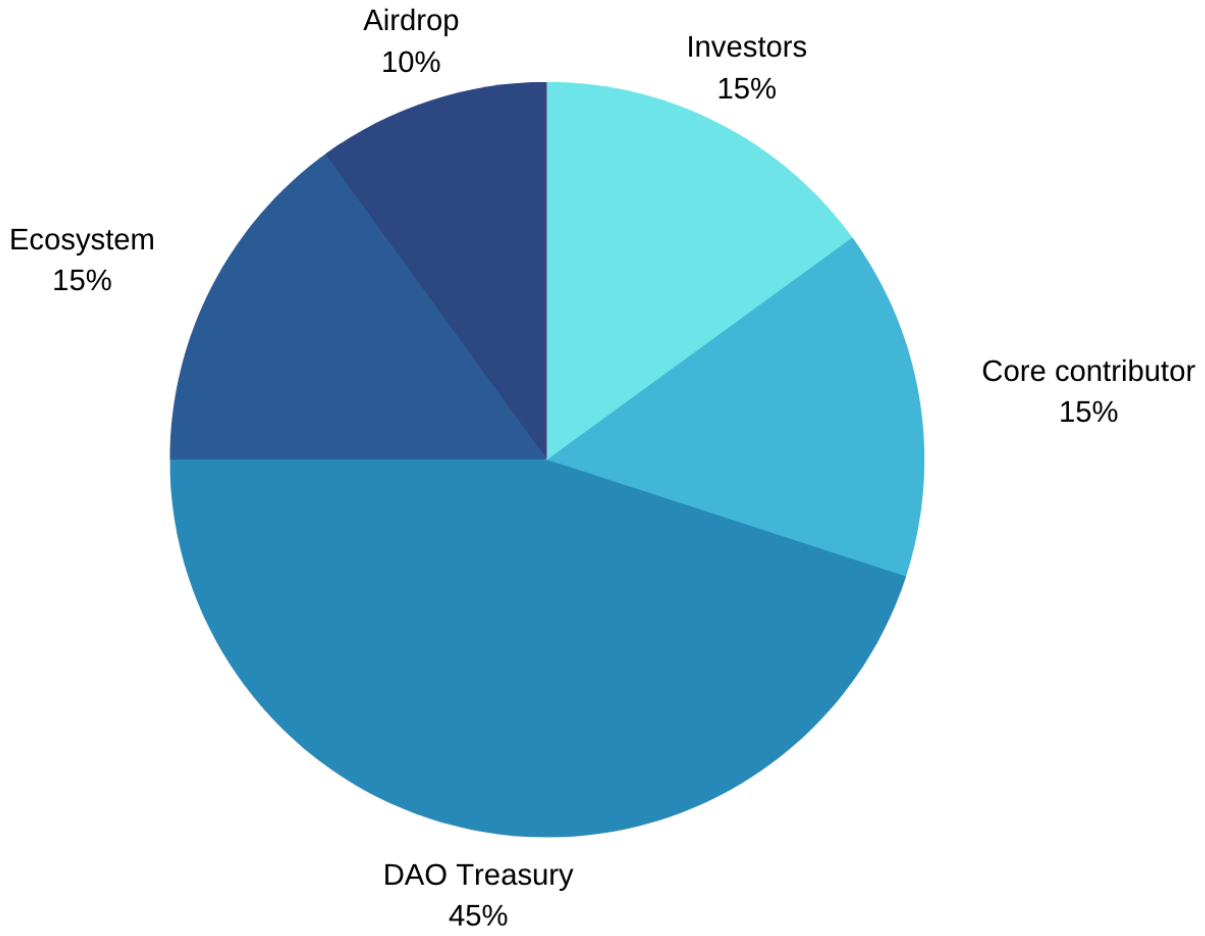
USD stable coin to pay for the cross-chain messaging. The cost of the messaging is determined by the payload size and the rate per byte set by the DAO for usage.

Tokenomics

Until our TGE, all governance and control of the CTMDAO Treasury is achieved through voting at https://snapshot.org/#/continuumdao.eth using a simple ERC20 token called CTMDAOVOTE on Polygon :- https://polygonscan.com/address/0x1FAaf080a77C421e833CdfCbDeaAa273f0eE23b5

Before TGE, the DAO will have a vote to decide which Core Contributors deserve their token allocations, since some left early or did not perform adequately. Other Core Contributors exceeded their targets and so deserve an increase in their allocation. At TGE, but subject to this vote, CTMDAOVOTE tokens will be converted 1:1 for veCTM, with the CTM locked for 4 years. The fixed Total Supply of CTM will be 100 million. At any rate, the total allocation to Core Contributors will not exceed 15% of the Total Supply (see below).

Allocation



▼ **DAO Treasury - 45%**

- The spending of the Treasury will be determined solely through on-chain voting using veCTM. The DAO, through voting, can allocate tokens for new projects, payment for services, or whatever they wish to, so long as it complies with the Mission and Vision statement in our Constitution.
- The Treasury will also hold tokens from other protocols. These could be projects that were incubated by ContinuumDAO, or other tokens (including RWA tokens) that were purchased on behalf of the DAO, or following DAO voting decisions to do so.

▼ **Ecosystem - 15%**

- Terms to be decided by DAO voting
- 5% allocated for chain partners
- 5% allocated for project partners

- 5% allocated for incubation incentives

▼ **Core contributors - 15%**

- 13% allocated for early core contributors. Core contributors will share this allocation as a veCTM token, with full voting rights at TGE.
- 2% allocated for future core contributors

▼ **Airdrop - 10%**

- 10% allocated for Airdrop for the early community who supported ContinuumDAO in its formation in 2023. The airdrop will be as a veCTM token, locked for 4 years and with full voting rights. These community members already hold CTMDAOVOTE tokens.

▼ **Investors - 15%**

- 15% allocated for VCs: The terms of any allocation to VCs will be determined by DAO voting, including a locking period.

Utility

- C3Caller cross-chain message payments (USD and other stable coins, CTM)
- Governance - as veCTM
- Staking to secure the MPC network - as veCTM
- Payment for staking on MPC nodes

Ecosystem Development

There will be a grant program for new projects using Continuum. This could be either a grant of CTM, or other tokens from the treasury, or a time-limited reduction in fees for usage of Continuum.

The DAO will assist new projects that wish to use Continuum. This will be in the form of coding support, joint marketing, and technical support as required. These functions will be undertaken and organised by the DAO Guilds.

AssetX is the first such project to receive support from ContinuumDAO, marking ContinuumDAO's entry into RWA tokenization. ContinuumDAO will be given 50% of the

AssetX Security tokens, once these Security tokens are minted (subject to gaining a Security License) and the Continuum MPC is fully decentralized and audited.

Lawracle is another project being jointly developed by ContinuumDAO. It is another service for RWA's, to create legal certainty around asset tokenization. Lawracle will provide on-chain proofs from law firms that asset tokens are really being backed by real assets and other statements made by web3 protocols are truthful. ContinuumDAO will be allocated 50% of Lawracle's token supply in return for technical services being provided by DAO members to build it.

This will be the model for the future. Any new protocol is free to use Continuum, without the involvement of the DAO, but some projects may wish to work directly with ContinuumDAO, leveraging its talent pool and grants. If the community decides to, through voting, then ContinuumDAO will form partnerships with some of these projects and take a stake of the new protocol for its Treasury. ContinuumDAO will pro-actively work to build usage of its cross-chain infrastructure and use the revenue from this to improve and extend the MPC network, to maintain a security reserve and to increase its reach.