ContinuumDAO

White Paper ContinuumDAO

8th September 2023

Introduction

The market for cross-chain messaging has grown enormously since 2022. It is currently dominated by Layer Zero, which received a valuation of $3B when its Series B round was filled by a group of VCs led by Andreessen Horowitz in April 2023. There is a clear need for alternatives to Layer Zero, which can be seen as just a 2/2 threshold security scheme (one being an oracle and the other a Relayer). Apart from this inherent lack of security, relying on only one solution for such an essential part of web3's architecture goes against its ethos. We believe that ContinuumDAO (CTMDAO) will set the standard for cross-chain security and versatility, with a messaging system that connects most non-EVMs and EVMs, is more secure, completely open-source, and verifiably decentralized.

The Position Statement in Appendix A makes the case for a more secure cross-chain messaging protocol, which will be created by ContinuumDAO. All currently available cross-chain protocols have serious security concerns, including reliance on attested multi-sig signatures that expose private keys and are vulnerable to attacks, where someone gains control of a threshold number of nodes (Wormhole, Axelar, Celer, Router), optimistic signatures with no visibility of how they work (Synapse), or 2-factor trust models that can be hacked by individual dApps (Layer Zero). Some protocols do not make their code and full security model public (Chainge, Synapse, Chainlink CCIP). SMPC (Secure Multi-Party Computation) networks can dramatically improve the security model, but only if they are implemented in a fully decentralized and transparent way, as we saw with the Multichain case, highlighting how important the governance of a protocol is.

The essential service that ContinuumDAO will offer is a state of the art peer to peer node network that will connect blockchains. Each node will join a set of others to collectively sign transactions using a Secure Multiple Party Computation (SMPC) based Threshold Signature Scheme (TSS).

The nodes, collectively known as the Continuum, will form a core part of web3 architecture for other protocols to use for applications such as a router, cross-chain messages, and NFT bridges. They will allow all EVMs and almost all non-EVMs to connect. The SMPC scheme will utilise the latest threshold signature algorithms, with a

lot of pre-computation, to deliver the fastest MPC network and signature sets far larger than those commonly used with MPC schemes to deliver extra security.

Of course, it is vital that all nodes in the network can be trusted to jointly sign transactions without any foul play. ContinuumDAO will run the network as a global DAO in a transparent way, with governance voting for decision-making built into the protocol at every level. To facilitate a truly trustless and verifiably decentralized architecture, the open-source code for nodes will be presented in a clear and well-documented way so that any decent cryptographer would have no trouble understanding it. The nodes in the Continuum will be chosen through on-chain governance following voting by the DAO, which will ensure that only trustworthy organisations or individuals are selected. Each node will log activity, and it will be possible to analyse which nodes in a set are used for each transaction.

Once the peer-to-peer SMPC network is running well, it will be converted into a blockchain, with blocks storing a ledger of all signing activity by nodes. Block rewards will be paid to those who run nodes and have staked tokens on their node.

Revenue Model

Other projects wishing to operate cross-chain will be able to use the message passing system without permission on each chain to send messages with data. They will be charged either on the source or destination chain per byte of data sent. Payment can be made in either the gas token of the chain or in CTM (our native token), with payment in CTM being slightly cheaper for the user. This will ensure high utility for the CTM token. Another revenue stream would be when projects choose to use Continuum, for instance our router, and they will be able to do so by either renting it or paying per use. CTM will charge a fee from the router, messaging protocol, and other services.

The DAO will serve as a launchpad for new projects developed on Continuum. This is expected to be a primary revenue source. The DAO may wholly or partially own new projects, thus receiving a share of their income stream, or may receive an allocation of tokens for the treasury. Continuum will be a fundamentally pure architecture, separate from the projects built on top of it. However, these dApps will be the main customer-facing projects, so it will be crucial to optimise their ability to funnel funds to ContinuumDAO.

To kick-start the ecosystem of projects built on top of Continuum, the DAO will launch the first dApp that employs the router to allow token transfers between several EVM and non-EVM blockchains. The Router project will be fully open source, allowing other customers to either fork it or integrate the router into their own projects.

ContinuumDAO

Governance Model

Governance roles

There will be three governance roles: Committee, Contributor, and Citizen.

- Committee will be responsible for signing transactions in multi-sig wallets that will perform asset transfers as directed by DAO voting.
- Contributors will include: node runners, Guild members, and core-contributors group.
- Citizens will have the right to join the governance process, which includes proposing, voting, and making contributions.

Committee

The CTMDAO committee will be responsible for signing transactions in multi-sig wallets that will perform asset transfers as directed by DAO voting. The Committee will 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 wholly or partially 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 to be included in the new veCTM token.

Contributors

To achieve the CTMDAO mission and vision, we need an amazing 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.

There will be a group of full-time contributors group in the DAO responsible for operating the server, official accounts, and other related tasks. The performance of the contributors will be reported each quarter in the DAO to evaluate.

ContinuumDAO

There will be 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.

DAO contributors will also receive additional voting power, dependent on how much they have added to ContinuumDAO using a Proof of Contribution stored in a smart contract.

DAO incentive system

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

- Full-time contributors and guild leader will receive monthly payment for the long-term stability and security of their work.
- Node runners will receive rewards based on their performance and other requirements.
- Guild members will receive payment based on the outcome of the guild missions.
- All people who have veCTM or a contribution history have the possibility to receive future airdrops with different percentages. The number will be based on the performance of their previous contribution history.

ContinuumDAO

Tokenomics

Vested Token Model

It will be possible to lock the project's token (called CTM) into an NFT called veCTM. All users who do so will earn a share of the revenue from the protocol. The share will be decided by the DAO, with the balance going to the DAO Treasury. Holders who lock for 4 years will earn the most per locked CTM, decreasing linearly to zero, as is common in many other DeFi protocols. Rewards will be paid in CTM at a rate to be determined by the DAO. Fees collected in native gas tokens will be used to buy CTM regularly by the DAO Committee and added to the smart contract CTM pool for rewards. In this way the available rewards for veCTM holders will dynamically reflect the Continuum usage. There will be a buy pressure for CTM to counteract any sell pressure from farmers selling tokens and the increased volume should benefit LP providers and attract DEXes to list CTM.

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. The splitting function will be subject to a small tax for the DAO. It will be possible to liquidate the 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 veCTM token will include OpenZeppelin Governance functions, so that voting can take place directly on tally.xyz This will present the option of controlling the Treasury and SMPC node selection/deselection using on-chain execution resulting from voting and following a time-lock period, during which it will be possible for the Committee to intervene to stop the execution. This is a temporary measure to be put in place until ContinuumDAO governance is more mature.

There will be a limited number of nodes in the Continuum. Each will be required to hold a veCTM with a threshold number of tokens locked. The DAO will perform node attachment through direct on-chain governance. Nodes will earn an enhanced share of the fees generated through their veCTM compared to ordinary unattached ones.

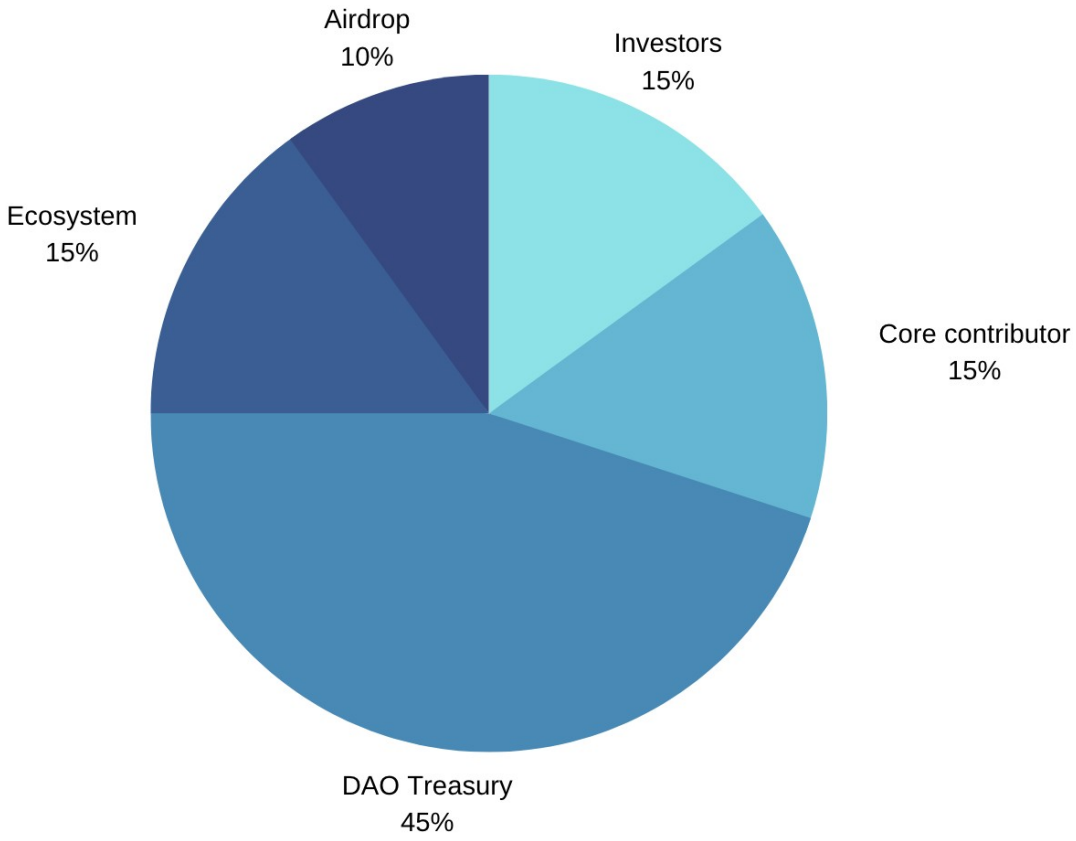
At some point, the DAO will commission a liquid staking token derived from the revenue earning veCTM, that can be traded as a normal ERC20.

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

ContinuumDAO

When the veCTM token contract is ready, 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.

Allocation



- **DAO Treasury - 45%**
  - 35% allocated to Treasury reserve
  - Allocated to nodes incentive
  - Allocated to contributors incentive
  - 10% allocated to initial support by MultiDAO as a veCTM locked for 4 years, but without voting rights.
- **Ecosystem - 15%**
  - 5% allocated for chain partners
  - 5% allocated for project partners
  - 5% allocated for incubation incentives

- **Core contributors - 15%**
  - 12% allocated for early core contributors. Each of these 4 core contributors will receive 2% as a veCTM token, with full voting rights and a further 1% as CTM with a locking period of 3 years and linear unlocking with 36 months
  - 3% allocated for future core contributors
- **Airdrop - 10%**
  - 10% allocated for Airdrop for veMULTI and MULTI holders. (Every veMULTI that has voted since the Compensation vote + anyone in the Early Steps Telegram Group who held MULTI on 14/07/2023). The airdrop will be as a veCTM token, locked for 4 years and with full voting rights.
- **Investors - 15%**
  - 15% allocated for VCs: The terms of any allocation to VCs will be determined by DAO voting, including a locking period.

Ecosystem Development

There will be a grant program for new projects using Continuum. This could be either a grant of CTM 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.

ContinuumDAO

Uses Cases

1. **Multi-signature asset management projects (MPC distributed wallet)**

   Multi-signature is another solution for ensuring fund security and management. However, due to its lack of compatibility (requiring deployment on a chain-by-chain basis) and the need for interaction with on-chain contracts, each operation requires verification of multiple user signatures, leading to increased gas costs for each transaction, especially on the Ethereum mainnet. Choosing the ctmMPC network ensures safety while allowing for one-time account application, compatibility with over 95% of chains, including EVM and non-EVM chains, and reducing transaction costs by over 60%.

2. **Distributed asset custody**

   Asset custody providers often directly use private keys for management, typically with isolation levels to ensure security, such as cold and hot wallets. However, the risks of this approach are obvious. There have been multiple instances of asset theft caused by the leakage of private keys by developers or internal personnel. Using MPC for asset custody protects the private key and prevents any malicious attacks. MPC is a secure multi-party computation technology that divides the private key into multiple pieces, allowing each node to only access part of the private key, thereby ensuring the security of the private key. This means that no single node or individual can independently control the private key, so even if some nodes are attacked, the security of the entire network will not be affected. In addition, MPC can also enhance the security of the custody network because it does not require trust in any single node, thus increasing user trust in the network. Therefore, choosing the MPC network for centralised exchanges and cross-chain bridges can provide high security for projects in the early stages.

3. **Distributed permission management**

   Currently, some project parties also adopt their own operated MPC networks, but those networks are either non-transparent or centrally controlled, more centralised, and will cause huge losses once attacked. If the Continuum is used and the MPC nodes are operated by multiple well-known web3 giants for product decentralization, not only will safety be guaranteed, but also the development of the entire Continuum MPC network ecology can be enjoyed.

ContinuumDAO

Appendix A Position Statement

We summarise here the main methods currently used to transfer value or messages between block chains. Each of these has security concerns that will be improved upon using our new SMPC network, combined with a DAO model with on-chain governance.

Layer Zero

The core security concept of Layer Zero is quite simple. It relies on an oracle, such as Chainlink and a relayer, which could be anyone, but in practice is usually operated by Layer Zero itself. The oracle waits for the source chain transaction to be finalised and then forwards the commitment of the message bundle such as a hash of the block header to the target chain and the relayer forwards a transaction proof, such as a Merkel proof to the target chain.

Issues:

- The trust network of Layer Zero is only two. If the oracle and the relayer collude, they can hack the system. As an example if the oracle header hash and the relayer proof are both invalid, but match, the system can be compromised.
- The security is only as strong as any one of the parts. Layer Zero security relies on the oracle's security, which has to be examined as part of the security assessment.
- It's up to the user application to provide the guarantees that the oracle and the relayer are honest actors. This is a burdensome task for a dApp. Alternatively, a dApp may choose to break the collusion guarantee. User dApps can choose their own oracle and relayer, or even switch to new ones at any time. Layer Zero is not secure by default. A bad actor with access to a dApp's code can hack the system.
- The relayer does not transmit a zero knowledge proof, which would be ideal and ensure security.

Conclusion:

Layer Zero has proven to be remarkably popular, at least between EVM chains, but its security is not optimal, being dependent on dApps to also be honest actors without the on-chain contract verifications that users so rely upon. There is no collective security mechanism for Layer Zero. As Layer Zero grows in popularity, it is inevitable that a bad dApp will eventually cause a hack that once again brings the entire cross-chain industry into disrepute.

ContinuumDAO

Wormhole

The security of Wormhole's network is dependent on Proof of Authority (POA). Wormhole is secured by a network of Guardians nodes that validate and sign messages. If a super majority (e.g. 13 out of 19) Guardians sign the same message, it is considered valid. The transaction is signed as a multi-signature on the target chain. The core smart contracts as well as any token bridge contracts can be re-deployed through governance with the same majority of nodes voting to do so. There is an internal blockchain called Governor, which is part of Cosmos. This can delay suspicious transfers.

Issues:

- There is a reliance on POA, so collusion to sign the multi-sig for a false message is possible.
- Running a node on each supported blockchain by each node is burdensome. It is hard to see how the Guardian network will scale by attracting more Guardian nodes, especially as new blockchains require support.
- Multi-sigs require a lot of gas and the more signatures required, the more expensive it gets. This will likely limit the willingness to increase the number of signatures and therefore Wormhole's security.
- Part of Wormhole's security proposition relies on Cosmos' Governor blockchain, so this has to be considered when evaluating risk.

Conclusion:

Wormhole is essentially a multi-sig solution to cross-chain transfers, with many of the known security implications of this approach.

Celer Network

A state Guardian network, based on a Tendermint blockchain receives a message, comprising of a structured header and binary data payload, from a dedicated smart contract on the source blockchain. The Guardian network reaches consensus via a stake-weighed multi-signature attestation and then transmits it to a another smart contract on the destination chain that checks the header for validity and then executes the message. The Guardian network relies on Proof of Stake (POS) for the voting attestation using the protocol's CELR token. There is an optional additional step to assist security, with a programmed optimistic-style delay on target chain execution, allowing for a watchtower service on the source chain to check the message consistency and prevent execution if desired.

Issues:

- The total value of CELR pledged on nodes is very low compared to the cross-chain volume, so there is an incentive to mount an attack by deploying malicious nodes.
- The Guardian network is similar to a multi-sig wallet signature. The private key to sign the target chain signature is exposed once attestation has been reached. This is a weakness and possible point of a hack.
- The additional optimistic-style delay shows that a majority attack is a possibility. That fact that the delay is optional means that the cross-chain security is weak by default.

Conclusion:

Celer is essentially a multi-sig solution to cross-chain transfers, with many of the known security implications of this approach.

Synapse Protocol

An optimistic verification system of cross-chain messages by a system of off-chain Guards is employed. Each of these Guards provides a proof that the message is valid. If there is only one honest actor, then the system will ensure security.

Issues:

- We do not know how many Guards there are, or who runs them.
- We do not have the source code for the off-chain Guards, so we cannot see how they operate.

Conclusion:

Synapse Guard code is not trustless, since we do not have the source code for the Guards and we do not have knowledge about who is running them, so we cannot say that the system is decentralized.

Router Protocol

There are Orchestrator nodes which use POS using the protocol's ROUTE token to vote on the validity of a cross-chain message. It is required that the threshold of 67% of the votes is passed to transmit the message from the source chain to the target chain.

Issues:

- The total market cap of ROUTE is very low compared to the cross-chain volume, so there is an incentive to mount an attack by deploying malicious nodes.
- The Orchestrator nodes are similar to a multi-sig wallet signature. The private key to sign the target chain signature is exposed once attestation has been reached. This is a weakness and possible point of a hack.

Conclusion:

Router protocol is essentially a multi-sig solution to cross-chain transfers, with many of the known security implications of this approach.

Axelar

Running their own Cosmos chain, there are about 50 validators, which vote using a quadratic voting scheme on whether to execute transactions from chain A to chain B. A two thirds majority is required to allow signing.

Issues:

- The voting is determined by how many AXL, the Axelar token is held by each node. Many nodes have only a small stake in the POS system, hence the need for quadratic voting.
- As with Celer, the total market cap of AXL is very low compared to the cross-chain volume, so there is an incentive to mount an attack by deploying malicious nodes.
- Once consensus has been achieved, the transactions are executed on the target chain, but it is not clear from their documentation if this uses a single private key whose very existence is a weak point, or what they allude to as an MPC scheme, but with no details about how this is achieved. If a single private key is used, then this is a weak point for attackers.
- Individual dApps can choose to use part of the validator network, thereby further reducing the security of the system.

Conclusion:

The documentation is not clear on how the details of how this bridge works and hence it cannot be considered trustless.

Chainge Finance

DCRM is an implementation of Multi Part Computation (MPC) that is used by Chainge for off-chain nodes to jointly create the private key to sign a transaction on a target

chain. The private key is split into shards, with individual nodes only ever knowing a piece of the private key for signing. The private key is never assembled. This is an example of a Threshold Signature, where a N nodes out of a subset of M nodes jointly sign the signature.

Issues:

- Chainge source code is not open source, so we cannot verify exactly how the DCRM nodes run.
- We do not know how many nodes there are, or who runs them. Conceivably they are all run by Chainge employees.
- We do not know if all of the nodes run in the same geographic location, with this possible inherent risk.
- There is no discussion regarding whether the Chainge nodes are checked to see that they are running a certified copy of the node software. There is no Trusted Execution Environment.
- Since we do not know anything about the nodes, we cannot verify which ones were involved in signing any particular transaction.

Conclusion:

Chainge DCRM may well be promising technology, but it is not trustless, since it is not open source, or verifiably decentralised.

Chainlink CCIP

Recently Chainlink introduced their Cross-Chain Interoperability Protocol (CCIP), which allows asset transfers and messaging between various block chains. Whilst CCIP does have the support of several banks in the legacy financial system, it is not a decentralised protocol, relying as it does on the SWIFT system implemented in various databases. Several countries are sanctioned from using SWIFT.

CCIP is not trustless, decentralised and is not open source.

ContinuumDAO

Multichain

Multichain deployed an MPC network of about 34 nodes. It employed a Threshold Signature algorithm to jointly sign transactions on target chains, with nodes only ever knowing a shard of the private key to do so. Multichain was working on a new fastMPC network on testnet, based on the latest GG20 MPC algorithm, when it ceased operation.

Issues:

- We have no knowledge of which nodes are used as part of the TS subset to sign transactions. We do not even know how the subset is selected.
- We don't have knowledge of which nodes signed particular transactions, so we are unable to identify any bad actors.
- There was no Trusted Execution Environment (TEE), so it was not clear that individual node software was unaltered by the node operator for particular malicious intent.
- The number of nodes in the TS may have been quite small, encouraging collusion, though this would be quite difficult to achieve in practise.

Conclusion:

The MPC code was open source and nodes were run by community members, but it seems that only a few nodes were actually used to sign transactions and these were all controlled by one of the co-founders. The use of MPC is the most technically advanced method of trustlessly signing transactions examined so far, since it does not depend on POS, POA and it does not expose any private keys. But it is only secure if it is deployed and operated with guarantees about the actual code running on nodes, with monitoring of message signing and node subset selection. The downfall of Multichain emphasises how important these guarantees are.