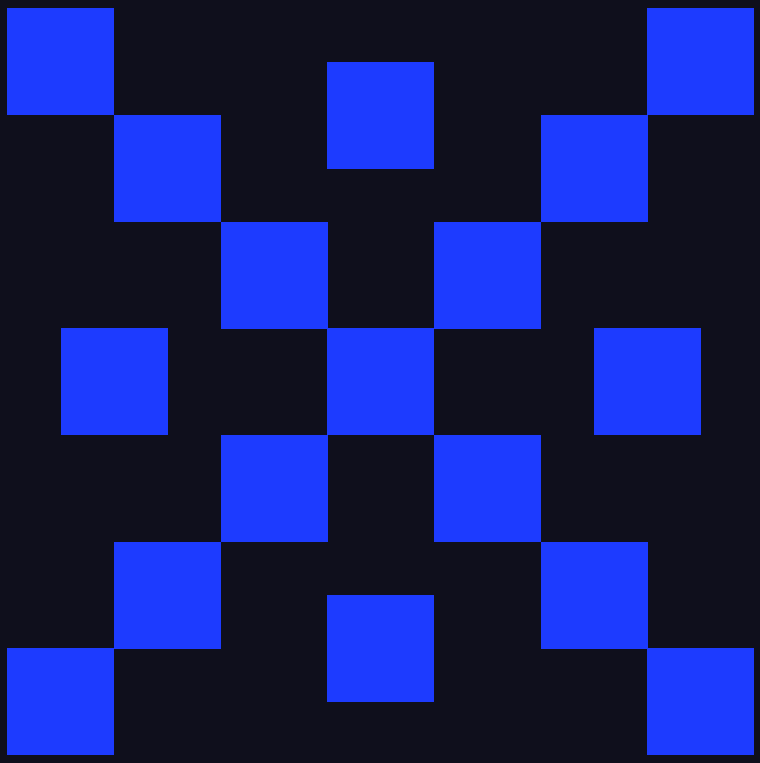


DCIPHER

A MODULAR NETWORK FOR THRESHOLD SIGNING

V1.0 MARCH 2025 | RANDAMU

INDEX

ABSTRACT

The last ten years in the crypto space have been characterized by tension between centralization and decentralization. Early bitcoin pioneers were set on the highest level of decentralization possible, seeing it as the only viable path to a future with peer-to-peer digital cash without government control. As networks grew in scale and capability, performance requirements necessitated projects such as Polygon to rely on weaker trust assumptions such as a smaller, permissioned validator set to optimize performance.

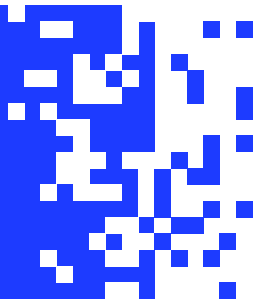
We believe the era of decentralization dogma is behind us - power should reside in the hands of dApp developers to choose the validator group size and composition most appropriate for their use case, without having to put all their 'eggs in one basket' of a single blockchain.

This paper presents a novel, modular protocol for committee formation and coming to consensus regarding data both on and off-chain, built atop threshold cryptographic primitives that are already widely deployed on blockchain networks.

Additionally, we detail a token-incentivized network deployment to implement the protocol at scale. This empowers dApp developers to define their own protocols and deploy them to hardware outside their direct control with whatever security guarantees they desire. We also articulate a roadmap to evolve from our current centralized offerings to a decentralized, community-owned ecosystem.

OUR VISION

2.1
THE VISION



We are building the foundational infrastructure to ensure fairness and integrity in decentralized decision-making — a critical component in safeguarding digital human rights. Our mission is to empower developers to create apps and services that are bias resistant, accountable, and verifiably equitable.

dcipher is our permissionless threshold network for signing that builds towards this mission. It leverages threshold cryptography to encrypt, verify, and notarize real-world data without trusting any single authority. As an engine for custom signing workflows, it enables a unified approach to achieving a spectrum of core functionalities — from reaching consensus over a computation to multi-party secret key distribution to re-encryption. The network's token-incentivized operators can dynamically form consensus committees to execute builtin or user-defined protocols on request, unlocking a new class of previously impossible applications.

Built on proven cryptographic techniques and a flexible protocol orchestration system, dcipher supports an extensive range of use cases — from MEV prevention and decentralized gaming to self-sovereign identity and DeFi. Using our protocol augments the security of existing systems, and strengthens with every additional operator, leveraging crypto-economic incentives to promote honest behavior among operators. In this way, our architecture not only scales with increasing application use but additively gains security over time.

Developers benefit from the flexibility to operate across blockchains, or independently, with the ability to configure security levels that match their specific needs — overcoming the inefficiencies and costs of traditional consensus mechanisms.

We believe that our novel design addresses three major gaps in existing threshold networks: centralized control, narrow functionality, and fragmented security. While many networks have been permissioned to mitigate risks, thus introducing centralization concerns, and are focused on just one function, dcipher is engineered for breadth — providing true decentralization, generalized capability, and compounding security.

2.2
HOW WE GOT HERE

As stewards of the League of Entropy and the drand project — a network providing verifiable randomness as a public good and the software powering it respectively —- we have long been acquainted with the resilience and reliability of operating real world threshold networks at scale, serving over 85 billion requests since drand's inception in 2018 with zero downtime.

Throughout drand's history, committee formation and management have been a pain point: standardized distributed key generation tools were limited and poorly specified, and ultimately our Kyber fork became an unofficial standard. Moreover, any desirable committee capabilities outside of generating randomness such as voting, disbursing tokens or ratifying new rules (e.g., what to do in the case of a network being shut down) required custom tooling, which caused us to resort to non-verifiable processes such as slack emoji voting.

In 2023, we launched the world's first practical timelock encryption scheme, tlock, on top of the drand network and built a suite of products with it such as Timevault, a tool for responsibly disclosing vulnerabilities in an assassination-proof way.

In building with tlock, we identified that there was an impedance mismatch between drand and the blockchain networks we wanted to work with: clock time and blockchain time aren't quite the same; a three-second network frequency didn't quite align with all chains at once; variations in cryptographic schemes between networks necessitated multiple drand networks. Partners in the ecosystem such as Sui ended up rolling their own verifiable randomness functions because of this impedance mismatch. We had dreams of using the same underlying technology for even more ambitious use cases such as orderbookless limit orders, timelock encrypted mempools preventing MEV, and 'Zapier for web3' automation tools, all without relying on a trusted executor.

Other threshold cryptographic protocols such as Lit Protocol, oracle protocols such as Chainlink, as well as teams building on trusted execution environments such as Blocky were achieving some of our goals in specific areas (access control and key management in the case of Lit, attesting off-chain data in the case of Blocky), we felt their lack of capabilities around committee formation, custom community plugin development, and a way to tie everything together into one holistic system left dApp developers unsupported.

All this led us to design the dcipher network: the world's first modular threshold network, allowing dApp developers to form their own committees, write and run their own signing, compute and decryption protocols, and bring any real-world data on-chain with verification, blurring the lines between what's possible on-chain versus off-chain.

2.3
WHAT WE HAVE TODAY

Instead of starting from ideological preconceptions or interesting technical problems, we've focused our development on building software that developers and dApp users actually want to use. We have enabled an entirely new type of blockchain application to be built by shipping a series of decentralized services and applications atop the following pillars:

2.3.1 Verifiable Randomness

Users and dApp developers can fetch publicly verifiable random numbers from our permissioned consortium of node operators in a manner similar to drand, but better aligned with the specifications of blockchain networks.

2.3.2 Timelock Encryption

Users can encrypt ciphertexts that can only be decrypted by our consortium of node operators once a given chain height has been reached on a specific blockchain. Users can even specify chain heights for blockchains other than the one they're operating on, laying the foundations for more sophisticated multi-chain workflows in the future.

2.3.2 Conditional Signing & Encryption

Our timelock encryption plugin sits in a more generalized threshold signing application that supports custom-built condition logic other than chain height. Our chain state plugin listens to smart contracts for updates and submits new transactions based on their state. This allows a variety of new event-driven paradigms for dApp developers to interact with their smart contracts without having to run their own services.

2.3.3 Computational Consensus

By relying on threshold signatures as an inexpensive form of consensus, we ship arbitrary computations to our consortium of operators using WASM and JavaScript and attest to their output on-chain without having to deal with the computational complexity of zero-knowledge proofs or infrastructural and operating complexity of trusted execution environments. For those that require it, integrating trusted execution environments with our approach would further enhance resilience and security through complementary protection mechanisms.

2.3.4 Re-encryption

Subscription services can encrypt content and gate access to it via our threshold network. Users who have paid for on-demand or subscription access have the content re-encrypted to their public key without the network ever seeing the underlying data. Coupled with decentralized storage, this allows for secure and permissionless filesharing, and creator platforms without the huge fees of incumbents.

2.4 WHERE WE'RE GOING NEXT

We've found a keen market of dApp developers for our on-chain services, but to fully realise our vision of pervasive committee tooling and a fully decentralized threshold network, we require research and development in a host of new areas.

2.4.1 Committee Formation

We've designed a suite of libraries and tools for forming committees that support distributed key generation (DKG) algorithms from the battle-tested Pedersen DKG to the bleeding edge high threshold, asynchronous variety whether working on the server-side, in the browser or on an edge device. Using them, you will be able to form committees, committees of committees, and mixed committees of single agents and committees, as well as fulfill common management functions such as updating membership, voting for motions, and sortition.

2.4.2 Bring-Your-Own-Oracle

Leveraging the computational consensus we've built already, we're dedicated to building a VM with built-ins for common tasks like making network calls and extensibility to enable developers to build their own precompiles for interacting with the outside world in ways other web3 tech can't, for example reading temperature sensors, interfacing with IoT devices, or interacting with AI models and multi-agent workflows.

2.4.3 Fully Permissionless Threshold Network

We believe these crypto-economic design decisions — coupled with solving some outstanding research problems — will enable us to run the first fully permissionless threshold network. This network can become a verifiability protocol for all other blockchains, combining the power of all validator sets into one.

THE NETWORK

3.1 ACTORS

Our network consists of the following actors:

3.1.1 dApp developers

dApp developers choose node operators at the price and trust level appropriate to their use case, form committees with them, and fund condition evaluation, computation, and signature generation over time.

3.1.2 dApp users

While dApp developers are the ones forming and funding the committees, dApp users may be the majority users. They interact with the dApps on-chain, and verify the results off-chain to ensure that both dApp developers and committee members have behaved honestly.

3.1.3 Node operators

Node operators provide hardware, stake collateral both to join the network and join a committee, and put their implicit reputation on the line through operation. They are rewarded for availability and for performing services to a given committee.

3.1.4 SLA police

To ensure a high quality of service, SLA police are stakeholders incentivized to watch node operator performance in committees, and submit proofs to the protocol when they think operators are operating below acceptable levels. These levels are governed at first through the Network Association, and later by the DAO.

3.1.5 Smart contracts

A host of smart contracts gate all access to the off-chain network in a verifiable manner. Node operators register their cryptographic material and terms of availability, dApp developers enter into contracts with node operators, and jobs are hosted and tracked for use by dApp users and verification by the SLA police.

3.2 SUPPORTED OPERATIONS

3.2.1 Operator onboarding and collateralization

Operators prove attribution of their public key and provide a base collateral to join the network. This ensures they can provide a minimum computational and financial capability to the network and serves as a disincentive against sybil attacks.

3.2.2 Price and availability configuration

Once onboarded, operators can set their availability for deals at discretionary price points and frequencies to derive an overall 'signing power'. Different jobs require varied compute requirements and frequencies of evaluation, for example checking a dead man's switch might only require infrequent evaluation, whereas checking the price of a real-world asset might require sub-second evaluation.

3.2.3 Deal negotiation

dApp developers choose operators that fit their requirements and formulate a deal at the highest price point of their chosen nodes. They submit it to the smart contract and operators must pick it up or risk a penalty. Deals have a fixed term, though may be refreshed with updated terms before the expiration providing all committee members agree.

3.2.4 Committee formation

Assuming a dApp developer has negotiated a deal with a party of operators, the operators engage in a distributed key generation protocol to agree on a shared committee public key and unknown secret key. They write the resulting public key with a valid group signature and send it back to the smart contract. A contract exists for each committee. dApp developers pay a small fee for forming the committee which is refunded from an operator's collateral if they fail to take part.

3.2.5 Deal funding

Users are not required to fund the entire life of their committee upfront, though are expected to maintain sufficient balance in the committee smart contract to keep it alive. Committee funding may happen on a different chain to the execution chain. If the balance of the committee smart contract dips below the required value to keep it alive, operators may sign an exit message, splitting the remaining balance and freeing them of committee obligations.

3.2.6 Deal renegotiation

When deals come close to expiry, they can be renegotiated at market rates to ensure continuity for smart contracts, while not locking operators into long-term contracts in uncertain market conditions, leading to poor reliability.

3.2.7 Workload definition and registration

A core component of each deal is the type of workload being performed. This may be a simple signing protocol such as signing a message periodically, a complex evaluation of real-world conditions such as chain state, execution of arbitrary code, or something else entirely. In the future, users will be able to register new workloads and conditions for their execution. These feed into availability and can be subject to protocol rewards, depending on demand.

3.2.8 Condition evaluation and signing

Condition evaluation and signing is the core of the protocol — the whole reason why committees are formed in the first place! Signatures are threshold signatures in order to attest a committee's agreement on a piece of data, observation, or belief. These signatures can be variously used as decryption keys, attestations, or as individual signatures in higher level committees. Condition evaluation details how an operator should come to agreement on a piece of data, observation or belief. Fundamentally, operators cannot be prevented from evaluating conditions using methods outside the terms of the protocol, but the machine-readable representation of these conditions forms the basis of the contract between dApp developer and dcipher network. In future, we envisage verifiable computations making up both the condition evaluation and the signing logic, making the network a protocol of protocols.

3.2.9 Re-encryption

Built on the same primitives as timelock encryption and conditional signing, users can specify conditions under which ciphertexts are re-encrypted for other users to orchestrate subscription services or send encrypted messages. This is done without the consortium ever seeing the underlying plaintext.

3.2.10 SLA police bounty hunting

To incentivize honest behavior, the SLA police look through historical partial signatures and complete signatures to identify anomalous windows of missed signatures. Should an operator be submitting signatures at a dangerously low rate — jeopardizing the likelihood of recovering a group signature for a given committee — SLA police can submit their findings to a punishment contract and confiscate some of the operator's collateral.

3.2.11 Operator offboarding

Operators can offboard their node should they wish to leave the network. This incurs a lockup time of two weeks to give time for SLA police members to crawl their historical transactions and identify anomalies for bounty hunting.

GOVERNANCE

Our vision detailed a future where threshold networks are open participation, democratic, and safeguard user sovereignty. In order to realize this vision, we've set a governance roadmap that will allow us to move fast in the early stages of the network while setting a clear path to decentralization and community management of the protocol and network in the near term.

4.1 THE THRESHOLD ASSOCIATION

The Threshold Association is a Swiss non-profit association that administers the initial Token Generation Event, token disbursements, grants programme, and early network operation until the mainnet is completely decentralized.

Its mandate is to stabilize the network, tune network parameters such as stake, excess availability and acceptable signing frequency in collaboration with the community for sustainability, and pave the way for the DAO to take over all its responsibilities once the network is self-sustaining. It may delegate some responsibilities — such as research and development — to other teams it deems competent as appropriate.

At a future point, which we envisage in approximately two years in the future, the Threshold Association will scale down its operation to a purely administrative one, create a proposal for its ongoing funding and have DAO members vote on it like any other proposal.

4.2 THE NETWORK DAO

The Network DAO is a digital autonomous organization composed of token holders of the dcipher network. After the Network Association scales down its operation and hands power over to the community, the community will make the majority of decisions regarding the future of the network. This includes, but is not limited to:

- Network crypto-economic incentives and disincentives;
- Network and protocol upgrades;
- Funding service providers for essential network services;
- Funding service providers for ongoing decentralization efforts;
- Funding bug bounty programmes.

For expedience, the DAO may appoint stakeholders to make decisions on their behalf, for example to remediate emergency security issues that require action in a manner faster than a DAO can reasonably vote on.

TOKENOMICS

5.1 WHY DOES THE WORLD NEED ANOTHER TOKEN?

First and foremost, the dcipher is an open-source project — just as with drand, users can use the software for free, fork and configure the code to their own preferences, and run their own custom networks. That said, we found with drand that many users wanted a stronger emphasis on out-of-the-box solutions with sensible defaults and easy integration points with other projects to avoid writing a host of custom adapters. With dcipher, rather than dictate functionality, we dictate only the rewards mechanism, liberating the plugin market from day 0 and creating a shared pool of operators to give users flexibility and convenience in a single network. Users can easily write plugins to extend the protocol's functionality while benefitting from the verifiability and modularity the primitives provide, offering hooks into all major blockchains. Developers can offer these plugins to others as free and open source, keep them entirely proprietary for their own usage, or monetize them through smart contracts. We believe every mode of operation has its place.

Therein lies why the world needs another token:

- To align the incentives for node operators running the dcipher network to act honestly and self-regulate, since threshold networks are not inherently permissionless without an incentive layer;
- To fund an ecosystem of developers to build tooling and plugins that will make the dcipher network more flexible and reliable;
- To pay for essential network services such agents verifying historical service level agreements, plugin development, and operator rewards;
- To decouple the network's value from other existing ecosystems, since it is by nature chain-agnostic and can be relied upon on any chain so long as the interfaces between it and the desired chain have been configured.

5.2 INCENTIVES AND DISINCENTIVES

5.2.1 Collateralization

Operators must first stake our native token to register as an operator within the network. This serves to disincentivize operators registering many identities in order to flood committees with their own nodes and take them over. If they advertise themselves as available then fail to join a committee, a portion of this collateral will be slashed. Should a critical amount of an operators' collateral be slashed, they are ejected from the network until they re-collateralize.

5.2.2 Rewarding Availability

To maintain a healthy, resilient network, we've designed a crypto-economic incentive system to ensure the network has capacity to process new jobs. Extra availability will give dApp developers diversity in the price point, ensure that operators are available to serve new requests, increase the reliability of operators on the network, and support sustainable network growth without wasting resources. Only a percentage of the lowest priced availability advertised will be rewarded. This, coupled with punishment for failing to join a committee disincentivizes actors from advertising unrealistic availability. This percentage is governed at first through the Network Association, and later by the DAO as described in the Governance section. Operators indicate their availability in terms of signing power and maximum evaluation capability, to ensure that they are not overloaded in times of high traffic.

5.2.3 Committee Formation

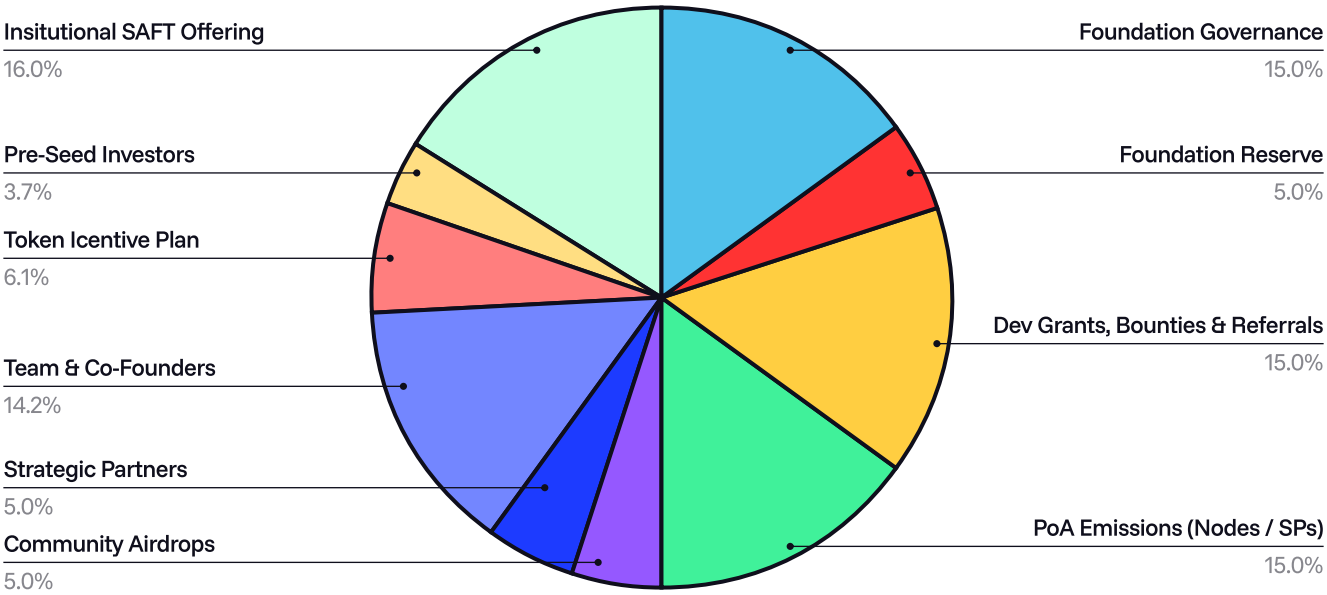
Users choose available operators to form a committee and pay money into a deal contract to kick off their committee formation protocol. A small fee is charged for this initial formation and should the formation fail, users are reimbursed through penalties paid from the collateral of non-compliant operators. Users set a signing and evaluation frequency for their conditions to determine the price.

5.2.4 Threshold Signing Game

Working with a leading crypto-economic research team, we've developed a game-theoretic basis for committee incentivization to make reliability tunable by users while ensuring that the network is correctly collateralized and gas isn't wasted. In committee formation, users tune the collateral level and rewards to ensure that high-stakes signatures are submitted or large punishments are levied, while operators don't need to waste gas submitting every single partial signature to get rewards.

5.3 PROPOSED TOKEN DISTRIBUTION

A more detailed token distribution can be found in the appendix.



ROADMAP

6.1 AREAS WE'RE TACKLING FIRST

The following areas are those where we see the most promise , and will be building custom systems on the dcipher network:

6.1.1 Verifiable Randomness

Anybody can run a drand network... but in practice few people have the time or expertise needed to do so, thus they rely upon the League of Entropy. We want to extend upon the great work of Anyrand and bring randomness to the masses, not solely with the League of Entropy, but with any committee you wish. We believe many companies will benefit from slashing their fees by running custom committees for randomness.

6.1.2 Distributed Validator Technology

By 2028, we believe a supermajority of Ethereum validators will be running as part of threshold validator clusters. Through our work together with SSV, we've seen that the reliability of distributed validators blows single-party validators out of the water. Coupling this resilience with restaking to repurpose compute through platforms such as Eigenlayer will crush inefficiencies in network validation and bring greater security to all chains. Distributed validators are simply a specialized form of committee, and our technology is already making them easier to create and more interoperable.

6.1.3 Sealed Bid Auctions for Oracle Data

As the concrete has set on the oracle space, the profitable companies are making much of their gains through priority access to data feeds in a form of 'oracle extractable value'. Many of the oracle providers are operating both the feeds and the sealed bid auctions, opening up potential avenues for attack or betrayal. By relying on a separate committee, trust can be spread amongst unaffiliated parties and increase assurance that the auctions are taking place fairly.

6.1.4 Timelock-encrypted Mempool for MEV Prevention

2024 was the year of the L2, with hundreds of new generalized and application-specific blockchains popping up, leveraging toolkits such as the OP stack and Scroll. Alongside it, a renewed appetite for experimenting with protocol-level features was born. While the notion of creating a new mempool for established protocols such as Ethereum mainnet seems ambitious, it's now trivial on L2s.

In launching an encrypted mempool module for the dcipher network, we believe the exploitation of retail DeFi traders will soon be coming to an end. If our experiments succeed, perhaps we'll see it on Ethereum mainnet in the future.

6.1.5 On-chain access control

Managing access, subscriptions and payments is a solved problem in the web2 space: there are many companies offering out-of-the-box solutions to all the headaches. Not so in web3: on-chain subscriptions have poor privacy, cross-chain access control requires maintaining many wallets and balancing them correctly, and payment flows are error prone and rely on centralized counterparties. Unified standards for threshold cryptography and custom committees simplify this by taking assets and state into chain-purgatory, allowing it to resurface on the relevant chains as necessary.

6.2 TECHNICAL TIMELINE

March 2025

Furnace testnet launched

Including randomness and timelock encryption, and PoCs of conditional signing and computational consensus

March 2025

Timelock Encryption launched on Filecoin

On Filecoin Calibration testnet

March 2025

Asynchronous DKG CLI and rust library launched

March 2025

Conditional Signing v1 launched

On Furnace testnet

April - July 2025

Randomness launched on BNB, Arbitrum, Polygon, OP, Base, Avax, Solana and Sui

On testnets

April - July 2025

Timelock Encryption launched on BNB, Arbitrum, Polygon, OP, Base, Avax, Solana and Sui

On testnets

April - July 2025

Promotion of Timelock Encryption on BNB, Arbitrum, Polygon, OP, Base, Avax, Solana and Sui

To Mainnets

May 2025

Gaming SDK released

Encapsulating functionality of randomness, timelock encryption, conditional signing

May 2025

Voting tool based on DKG CLI launched

May 2025

Limited re-encryption capabilities launched

Re-encrypting chain state; no adapters to external off-chain state. On Furnace testnet

June 2025

Computational Consensus launched

On Furnace testnet

June 2025

Multi-operator registration and collateral contract testnet launch

Managed by Randamu, permissioned

June 2025

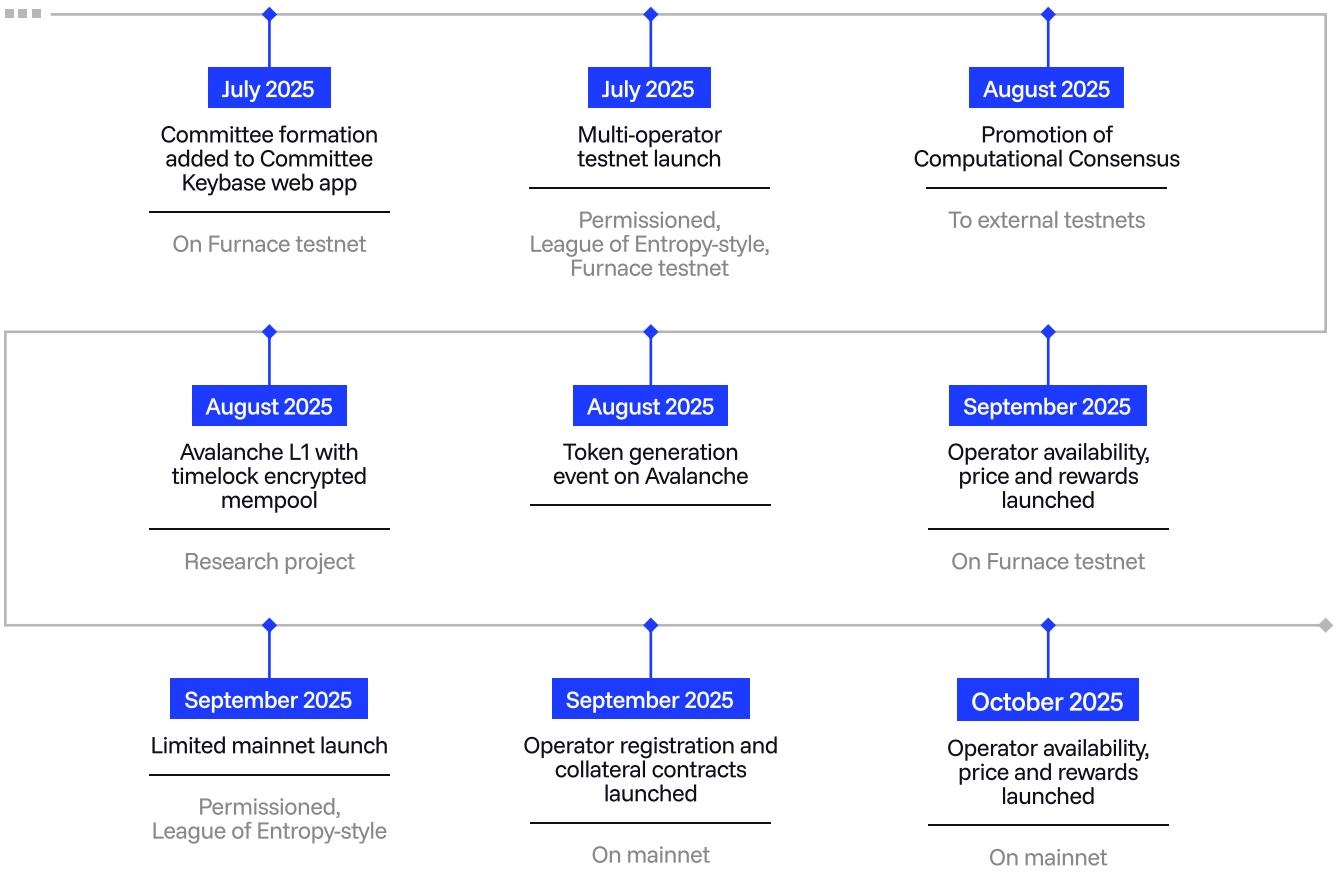
Deal negotiation for a single committee live

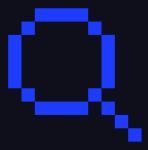
On Furnace testnet

July 2025

CommitteeKeybase web app launched

On Furnace testnet


July 2025
Committee formation added to Committee Keybase web app
On Furnace testnet
July 2025
Multi-operator testnet launch
Permissioned, League of Entropy-style, Furnace testnet
August 2025
Promotion of Computational Consensus
To external testnets
August 2025
Avalanche L1 with timelock encrypted mempool
Research project
August 2025
Token generation event on Avalanche
September 2025
Operator availability, price and rewards launched
On Furnace testnet
September 2025
Limited mainnet launch
Permissioned, League of Entropy-style
September 2025
Operator registration and collateral contracts launched
On mainnet
October 2025
Operator availability, price and rewards launched
On mainnet



AREAS OF FURTHER RESEARCH

7.1 TRAITOR TRACING

One of the biggest apparent weaknesses of threshold cryptography is the fact that compromise can be silent. If the majority of bitcoin miners collude to mine invalid blocks, anybody can post facto verify the transactions and see this to be the case; if the majority of members of a committee collude to recover the committee secret key they can use it for malicious purposes and it's impossible — outside of real-world investigative work — to identify which of the parties colluded, and who is using the recovered secret key. There are cryptographic schemes for identifying individual traitors, but identifying a colluding majority is an open research problem. We believe there are crypto-economic ways to disincentivize collusion that are as yet untested given the lack of large scale decentralized threshold networks in the wild. Through the dcipher network, we intend to publish foundational research in this space.

7.2
THE METACOMMITTEE

In the sections on committee formation, we briefly addressed the notion that committees could be composed of individuals and other committees. Like traitor tracing, the literature on and practical implementation of this is limited in the wild. There could be a role for metacommittees in attributing levels of assurance to claims: one committee reaching agreement on a claim could provide reasonable assurance for a low-stakes case, and all the committees agreeing on a claim providing a much higher level of assurance for higher-stakes use cases. Additionally, we believe cross-committee interaction opens the doors to new reputation systems, such as proof of service: dcipher operators could opt in to providing services to web2 customers as part of a committee, while being tested by members of other committees for availability and honesty. Despite interactions taking place off-chain, consensus can be reached and verified on-chain for rewards or penalties.

GLOSSARY

AVAILABILITY

The capacity of operators across the network to perform a given job.

Excess Availability

A small percentage of non-committed availability is incentivized amongst operators to promote competitive pricing of jobs, reliability of operators and sustainable network growth.

Operator Availability

Operators provide resources to fulfil a given job under conditions they set for the cost per signature and maximum signing frequency.

Operators commit availability for a set duration on becoming a signer within a committee. Active committees therefore occupy a given amount of 'signing power' of the network.

COLLATERAL

Registration Collateral

A stake of dcipher tokens made by operators when registering on the network, of which a certain percentage must be maintained to remain part of the network. Stake can be slashed for refusing to join deals that meet an operator's conditions.

Deal Collateral

A stake of dcipher tokens made by operators when forming a new committee. Stake can be slashed for sub-optimal or malicious behavior.

COMMITTEE

A set of signers, with a shared distributed key set, bound by one or more deal contracts. Committees are responsible for performing threshold cryptography jobs in an efficient manner.

Committee Members

See signers.

Committee List

A list of active and inactive committees, their members, and their public key.

Meta Committee

A committee acting as a signer within another committee.

COMPUTATIONAL CONSENSUS

A cryptographic signature from a committee attesting to agreement on the output of a computation that a threshold number of signers have verifiably executed.

CONDITIONAL SIGNING

A cryptographic signature workflow in which a threshold number of signers in a committee attest to a certain condition being met - such as a given time elapsing, a data input being received, or a computational result being achieved.

DEAL

A fixed term smart contract in which developers define a job to be carried out, a member list to undertake the work, and conditions under which the work must be completed - for example costs of evaluations or computations, a minimum signing frequency and a maximum signing cost.

Deal costs are paid for by the developer, as are committee formation fees where necessary.

Deals can be renegotiated close to expiry provided all participants agree on updated terms.

Deal Member List

A list of operators requested to participate in a deal. This can be expressed as an existing (already formed) committee, an exact list of operators to form a new committee, a list of committees, a list of operators that are deemed to have met certain conditions (availability for job types, cost, membership period, identity characteristics: operational jurisdiction, type of controlling entity, etc) or any combination of the above.

DEVELOPERS

Define deals and fund committee formations, condition evaluations, computations, and signature generations. Developers make jobs available to users through dApps and their results can be verified off-chain.

DCIPHER NETWORK

A permissionless threshold cryptography network for custom signing workflows. It consists of on-chain components, including smart contracts, an off-chain network, and some off-chain tooling and libraries to support easy interaction with the network for developers and operators. Pronounced dee-cipher.

$dcipher Token

Network token used to incentivise optimal behavior of operators on the network and to punish malicious or inefficient behavior.

dcipher Improvement Process (DIP)

The dcipher Improvement Process (DIP) is a community-driven framework used to propose, discuss, and implement changes to the dcipher network. Inspired by improvement processes in other blockchain ecosystems, DIPs provide a standardized way for stakeholders to contribute to the network's evolution, ensuring transparency and decentralization in its governance.

DISTRIBUTED KEY GENERATION (DKG)

A cryptographic process in which multiple parties contribute to the calculation of a shared public and private key set that can be used for encryption, attestations, or data signing without any single party having access to the shared private key.

DISTRIBUTED VALIDATOR TECHNOLOGY

Cryptographic operations and responsibilities of blockchain validation split across a committee, enhancing resilience, reliability, efficiency and security.

EMBERS

Executable code, packaged in WASM format, to be run, and verifiably completed, by signers as part of a job.

FURNACE

The network testnet.

JOB

A computational operation that can be assigned to a committee and undertaken by signers. Given successful completion of the operation, a signer generates a partial signature.

A job can have conditions for completion (time, on result, …), evaluation (source, frequency, evaluation type, failure modes, ...), computation (source, frequency, expected result type, ...) and signature generation (trigger, time, result, etc).

Jobs are carried out at a cost and frequency defined in a deal between a developer and the committee.

OPERATOR

Provide computational resources to the network. Operators advertise their availability so that they can become signers as members of a committee.

Operator Address

When registering on the network, operators provide an address anchored in a Verifiable Data Registry (blockchain, web domain, sidetree, KERI etc), which is published on multiple mediums. By being anchored in a VDR operators can cryptographically provide proofs.

RE-ENCRYPTION

A cryptographic process by which a ciphertext can be encrypted by a threshold network with a new key without revealing the underlying plaintext. It enables secure cross context data sharing without compromising confidentiality or requiring trust in a central authority.

REWARDS

Availability rewards

Token rewards given to operators based on their advertised availability and current committee membership to incentivize network capacity at competitive prices.

Policing rewards

Token rewards, taken from operator collateral and given to operators or users for reporting sub-optimal or malicious behavior on the network.

SIGNER

A member of a committee, that could be an individual operator or another committee, that is responsible for completing assigned jobs. To ensure efficiency in the network not all signers within a committee perform assigned jobs every time they are due to be executed. Signers can be nominated by developers who pay to form committees. When joining a committee signers put up collateral against their claims for availability. They are incentivized to behave honestly and ensure that signing thresholds are met, without wasting gas, otherwise their collateral is slashed.

SLA

Service level agreement. A certain service level is expected given optimal behavior of operators in the network and can be evaluated against a probabilistic distribution.

SLA Police

Any user or operator can monitor the behavior of committees, or other operators. Behavior is policed by submitting a report that demonstrates suboptimal behavior; users can be reimbursed for unfulfilled jobs and operators can confiscate operator collateral.

THE NETWORK DAO

A digital autonomous organization composed of token holders, responsible for making decisions about the future of the network.

THE THRESHOLD ASSOCIATION

A Swiss non-profit association that administers the initial token generation event, token disbursements, grants programme, and early network operation until the decentralized mainnet has been launched and the Network DAO has been formed.

THRESHOLD CRYPTOGRAPHY

Cryptographic techniques that distributes operations across multiple parties, requiring a minimum number (threshold) of participants to collaborate for the operation to succeed. Eliminating single points of failure, enhancing security by preventing any individual from having complete control, and enabling sophisticated conditional logic across decentralized systems.

THRESHOLD NETWORK

A decentralized infrastructure where cryptographic operations require collaboration from a minimum subset (threshold) of network participants rather than a single entity. This architecture creates resilience against attacks and censorship while maintaining operational integrity even if some network participants become compromised or unavailable.

USERS

Search for and request jobs to be fulfilled through developer dApps.

WORKLOAD

The total computational effort required by a committee over a given period. It is calculated as the product of the number of jobs, and their conditions, performed by the committee and the frequency at which these are performed.

DISCLAIMER

The present light paper and/or any other accompanying documentation (''Document”) only provide educational material about the Threshold Network and its utility token. Please note that the Threshold Network and the token are under active development and are subject to change. The Threshold Association, in formation, may change this Document at any time at its sole discretion without notice.

Any documentation is provided for informational purposes only and does not constitute some kind of prospectus, key information document or similar document. No prospectus, key information document or similar document will be provided at any time. There is no guarantee for the completeness of the documentation provided. All numbers and forward-looking statements mentioned within the present document as well as any accompanying documentation reflect mere estimations/indications. They are not guaranteed and may change substantially.

Any and all liability of the Threshold Association, in formation, and/or any affiliated legal entity or private individual for the completeness and accuracy of the documentation provided and any damages arising from reliance on such documentation is limited to the fullest extent permitted by any applicable law.

Any dispute related to or arising out of the information provided within the present Document as well as any accompanying documentation shall be submitted to the exclusive jurisdiction of the competent courts of Zug, Switzerland, with the exclusion of any other jurisdiction or arbitration.

This disclaimer, the Document as well as any accompanying documentation shall be governed by and construed and interpreted in accordance with the substantive laws of Switzerland, excluding the Swiss conflict of law rules. The United Nations Convention for the International Sales of Goods is excluded.

APPENDIX

Controlled by	Category	Description	%	Tokens	Vest Yrs.	1	2	3	4	5	6	7	8
Community	Foundation Governance	Holdback for future issuance, burning programs, other TBD uses. 20 - 40% (incl. Reserve) is considered 'standard'.	15.000	1,500,000,000	8	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000
Community	Foundation Reserve	Rainy day fund for 'unknown unknowns'. (Legal defense fund, etc.) Typically 5%.	5.000	500,000,000	0	0	0	0	0	0	0	0	0
Community	Dev Grants, Bounties & Referrals	Attract & support devs to build & support dApps, infra, and tooling. Typically 25%	15.000	1,500,000,000	8	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000
Community	PoA Emissions (Nodes / SPs)	Algorithmic minting (not vesting) for Node Ops & SPs to provide the required infra. (Unique to dcipher.)	15.000	1,500,000,000	8	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000	187,500,000
Community	Community Airdrops	Phased quarterly releases in Yr. 1 for sustained launch engagement. Typically 5%.	5.000	500,000,000	1	500,000,000	0	0	0	0	0	0	0
Community	Strategic Partners	Strategic Partners who bring liquidity, tokens & fiat to the table. (Ex. CEL, DEX's, DIA Data, etc.) Typically 5%.	5.000	500,000,000	4	125,000,000	125,000,000	125,000,000	125,000,000	0	0	0	0
Community	Team & Co-Founders	1 yr. cliff + 3 yr. vesting to retain key contributors. (4 yrs. total) 7.5-15% is considered 'standard'.	14.200	1,420,000,000	4	355,000,000	355,000,000	355,000,000	355,000,000	0	0	0	0
Community	Token Incentive Plan	Holdback for future employees & partners. Typically 5-10%	6.116	611,600,000	4	152,900,000	152,900,000	152,900,000	152,900,000	0	0	0	0
Community	Pre-Seed Investors	Pre-Seed Investors = 6mo. (15%) cliff then monthly for 18 mo. (2 yrs total).	3.684	368,400,000	4	184,200,000	184,200,000	0	0	0	0	0	0
Company	Institutional SAFT Offering	SAFT Offering / SAFT Investors = 12mo. cliff + monthly @ 24mo. (3 yrs total).	16.000	1,600,000,000	2	533,333,333	533,333,333	533,333,333	0	0	0	0	0
Company	INITIAL SUPPLY		100.000	10,000,000,000	3								


dcipher
NETWORK