Tangle Network: An MPC-as-a-service blockchain restaking infrastructure.

Webb Team

hello@webb.tools

March 28, 2024

Abstract

This paper introduces the Tangle Network, a restaking platform designed to support cross-chain and zero-knowledge (ZK) applications. Built on the Substrate blockchain framework, the Tangle Network provides a variety of multi-party computation primitives on-demand to power privacy-enhancing zero-knowledge applications, cross-chain applications, and other complex cryptographically secure decentralized applications. Tangle is built around restaking, enabling staked validators from its own and other networks the ability to provide MPC services for paying customers over a decentralized network and earn rewards in the process. The network's restaking primitive combined with MPC services enables an outsourced and crypto-economically secured services provider.

Contents

1 Introduction

In the rapidly evolving landscape of blockchain technology, several pressing challenges have emerged, notably the issues of interoperability, development limitations, governance inefficiencies, and privacy concerns. Traditional blockchains often operate in isolation, creating fragmented ecosystems that hinder seamless collaboration. Furthermore, the limited toolsets available to developers and the absence of robust cryptographic security measures in governance have curtailed the potential of many decentralized systems. The Tangle Network, built upon the advanced Substrate framework, addresses these challenges head-on. Designed to facilitate new Zero-Knowledge (ZK) applications that even interoperate across blockchain networks, it offers unparalleled interoperability, enhanced privacy functionalities, and a sophisticated governance model underpinned by a Distributed Key Generation (DKG) protocol. This whitepaper delves into the innovative solutions offered by the Tangle Network, showcasing its potential to redefine the standards of the blockchain industry and lay the groundwork for a more interconnected, secure, and user-centric decentralized future.

2 Vision & Motivation

The core vision of Tangle is to reduce the friction of deploying advanced cryptographic and zero-knowledge applications in production. We aim to expand the frontier of possible zero-knowledge application space by combining cross-chain interoperability with zero-knowledge and privacy-preserving tools. Our zero-knowledge messaging infrastructure based on threshold signatures and light-clients allows private data transfer across many EVM compatible blockchain ecosystems. Additionally, wae enable cross-chain governance through the use of various DKG protocols that interoperate with the plethora of signature schemes available on other blockchains. We reduce the friction of operating and deploying zero-knowledge applications by leveraging various MPCs to handle proof generation and trusted setup generation. Together, we empower developers to build the next thousands of zero-knowledge applications in production by eliminating operational burdens that slow down production deployment of zero-knowledge applications, cross-chain applications, and applications at this intersection.

As the research and infrastructural landscape develops, Tangle will continue to innovate and augment its service offering to reduce as much friction as possible. Today we see proof generation and trusted setups as being one core piece of friction for fast production deployments of zero-knowledge applications. Other areas of friction include witness generation, data storage, and key management. We believe MPC and other privacy-preserving technologies play a huge role in alleviating these frictions to provide seamless user experiences for zero-knowledge applications.

3 Background

3.1 Secure Multi-party Computation (MPC) protocols

Secure multi-party computation is a cryptographic field with the goal of designing protocols for multiple parties to jointly compute functions over inputs while keeping many if not all of those inputs private. The functions of interest are vast and span a variety of topics from cryptography to machine learnings. Examples of such protocols are distributed key generation (DKG) where the goal is to compute a shared public-private keypair to federated learning where the goal is to train a machine learning model of privately held data.

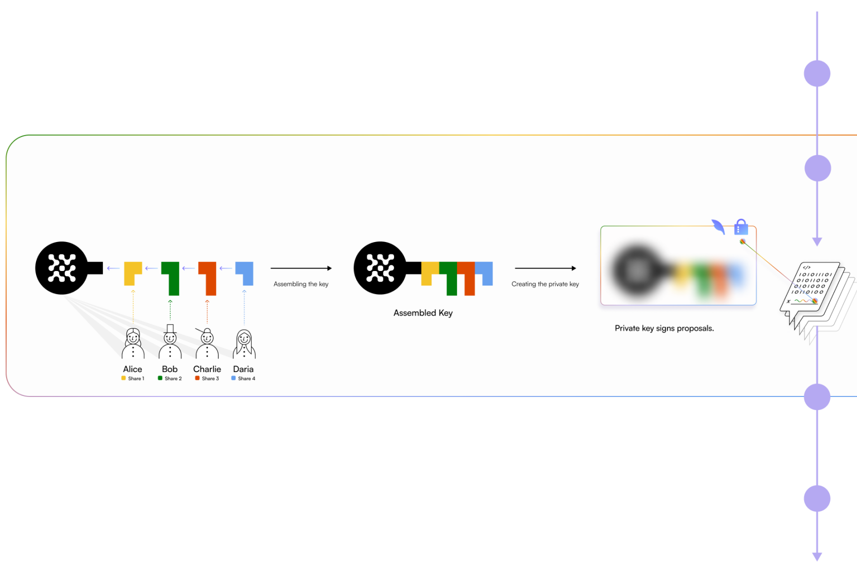

Figure 1: An example of the Threshold Signature Scheme offered in Tangle Network.

MPC protocols rely heavily on certain primitives such as secret sharing [16] which enable inputs to be securely distributed amongst the multiple parties in a privacy-preserving manner so that they can then be computed on, using standard arithmetic operations like addition and multiplication.

3.2 Distributed Key Generation (DKG) protocol

DKG, first introduced by Torben Pedersen in 1991, is a protocol that enables multiple parties to collectively generate a shared public-private key pair [14]. During the process, each party obtains a share of the private key, but the entire private key is never formed in any single location. Therefore, this method provides robust security against single point failure and adversarial attacks.

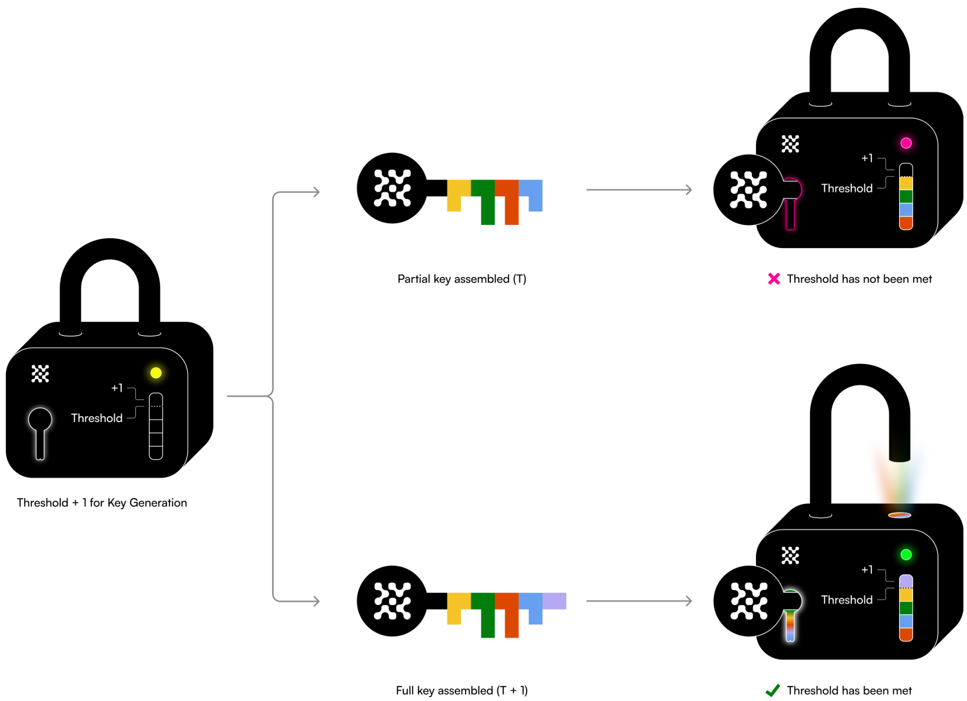

Figure 2: Distributed Key Generation analogized with keys broken into multiple shards.

DKG offers a highly democratic method for creating shared keys. It can be used in various multi-party computation applications, such as threshold signatures, secure multiparty lotteries, and secure multi-party blockchain validation.
We leverage DKG to power our cross-chain and governance infrastructure, since it provides a trust-minimized way to decentralize operations over a variety of applications and protocols on smart contract blockchains.

3.3 Zero-knowledge proofs

A zero-knowledge proof (ZKP) is a cryptographic method that allows one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement. It is a powerful tool in cryptography that enables the verification of information without disclosing the underlying data, providing a high level of security and privacy. ZKPs are used in various real-world applications, such as blockchain technology, where they allow

for the verification of transactions without revealing sensitive information, and in scenarios where users want to prove their identity without disclosing personal information. The three fundamental characteristics that define a ZKP are completeness, soundness, and zero-knowledge.
In the context of zero-knowledge proofs (ZKPs), completeness, soundness, and zero-knowledge are fundamental properties that define the reliability and privacy of the proof system.

- Completeness: This property ensures that if the statement being proved is true, an honest verifier will be convinced of its truth by an honest prover. In other words, the proof system should accept true statements with high probability when both the prover and verifier follow the protocol correctly.
- Soundness: Soundness guarantees that a dishonest prover cannot convince the verifier of a false statement. If the statement is indeed false, the prover should not be able to persuade the verifier, except with a negligible probability of error.
- Zero-knowledge: Zero-knowledge refers to the privacy aspect of the proof. It ensures that even after interacting with the prover, the verifier learns nothing about the secret information other than the fact that the statement is true. The prover does not reveal any information that could be used to reconstruct the secret.

These properties are essential for ensuring the reliability, privacy, and security of zero-knowledge proofs in various cryptographic applications.

4 MPC-as-a-service (MaaS)

Tangle's unique offering centers around its multi-party computation protocols. The core protocol leverages the underlying validator set to provide different computations as a service for the purpose of aiding developers in the deployment and operation of advanced cryptographic applications. We use *restaking* introduced by Eigenlayer [19] wherein validators restake their locked stake in additional computational tasks. For completing these tasks, validators earn additional rewards, and for failing to complete or maliciously disrupting tasks, validators lose their stake through slashing.
The protocol's validator set runs these protocols on demand to provide services that target cryptographic and zero-knowledge applications. Validators gain reputation and rewards by participating in computations and can opt-in and out of different roles that provide different services.
The core service offering is geared towards cryptographic applications, namely zero-knowledge application development. We aim to eliminate as much friction as possible in the design and development of cutting edge zero-knowledge applications as well as their production deployments. Our infrastructure additionally provides primitives for other advanced cryptographic applications like oracles and custody solutions. The network aims to fulfill on the following MPC primitives:

- Signing as a service
- Proof generation as a service
- Trusted Setup generation as a service
- Encryption/Decryption as a service
- Random number generation as a service

- General MPC as a service

An instance of one of the MPC primitives is often referred to as a service. That is, a user will request a threshold signature scheme (or signing) as a service (TSSaaS) which includes a distributed key generation and one or more executions of a threshold signature protocol to generate digital signatures. The two or more phases of this interaction is referred to as a service. The individual components of a service (the DKG / TSS) are referred to as jobs. Together, the MPCaaS offering provides job requests and submissions for a growing number of multi-party computation protocols.

The next sections describe the various specific MPCaaS protocols Tangle is focused on providing.

5 Signing as a service (TSSaaS)

Signatures are pervasive in the design of blockchain bridges, oracles, and custody solutions. Tangle provides signatures as a service using threshold cryptography as a first-class citizen of the protocol. Validators are selected to participate each session in a multi-party distributed key generation protocol, perhaps multiple, in order to create a key used for threshold signing.
Application developers can leverage signatures over custom payloads to design both private and non-private cross-chain applications. Tangle's relayer infrastructure handles message passing between connected applications and fits into any application architecture needed.

5.1 *Use Case*: Bridges and oracles

Tangle's distributed network of validators can be used to act as oracles over offchain and onchain datasets, providing cryptocurrency price feeds or onchain contract events from other blockchains to one another. These primitives form the backbone of more complex applications such as bridges. Tangle's native light-clients enable a hybrid trustless model for onchain oracle based and bridged applications.

5.1.1 Onchain oracles and zkOracles

As described in later sections, Tangle comes equipped with trustless light clients to other protocols such as Ethereum mainnet as well as the Cosmos and Polkadot ecosystems. This enables the trustless proving of events from these chains on Tangle. Having this ability as a native feature of Tangle enables developers easy access to block headers for oracle proofs of onchain data and events.
Layering these primitives together enables developers to build trust-minimized bridges for data and assets across blockchain ecosystems. The DKG protocol secures the signing of these events by enforcing slashing over deviations.

5.2 *Use Case*: Interoperable Shielded Pools

The most immediate application is the creation and operation of private bridges for assets, otherwise described as cross-chain private transaction systems. The decentralized, updatable Tangle Network is ideal for maintaining the state of a set of bridged shielded pools since it was purpose built for Webb Protocol Anchor Systems [17]. The Anchor System provides an architecture for the design and implementation of varying types of private bridge protocols, for individual or multiple assets, and with varying extensions for the incorporation of identities, compliance features, and incentives. We describe different flavors of interoperable shielded pools made possible by the Anchor System.

5.2.1 Multi-asset shielded bridges

The multi-asset shielded pool and its bridged extensions are a compelling use case for Tangle's infrastructure. Also referred to as the Variable Multi Asset Anchor System, this system enables users with the ability transfer arbitrary amounts of different assets privately between blockchains. The Variable Asset Anchor System uses zero-knowledge proofs and is similar to a shielded UTXO system, but with cross-chain capabilities.

5.2.2 Identity-Based Variable Asset Anchor System

By combining an identity protocol and the Variable Multi Asset protocol, a cross-chain shielded pool application over a restricted identity set can be designed. This creates a private transaction system where only users with proofs of membership in a cross-chain identity system can transact. This opens up possibilities for compliance or community based private transaction systems.

5.3 *Use Case*: Social and Identity Bridges

With interoperable private state provided by extensions to Webb's Anchor System [17], cross-chain social and identity bridges can provide a much needed primitive that powers a variety of content and membership based applications. Application developers can design social networks and identity registries with customizable zero-knowledge proofs of membership. This enables unique experiences for posting content, voting, and organizing groups of identities across blockchain ecosystems.

5.3.1 Interoperable Membership Groups / Semaphores

Semaphore [10] is a popular zero-knowledge protocol that enables members of an on-chain community to create anonymous signals using zero-knowledge proofs of membership in the community's identity set. This concept can be extended to a cross-chain identity set, allowing any member of a set of non-fungible token (NFT) communities to register.
Interoperable membership groups are thus communities that exist across chains and leverage privacy preserving interactions for content creation, voting, and more. An example of such a system is an interoperable Semaphore system, where anyone in one-of-many Semaphore membership groups can cast a vote or respond to a poll from any chain privately, and potentially without even needing a wallet on that chain. Connecting communities with privacy features increases the level of privacy afforded to individuals in a single community.

5.3.2 Interoperable Badge System

Another identity-based application, an interoperable badge system, could use expressive data blobs for arbitrary proofs of ownership, participation, and identity. These badges can be proven to exist from any chain and contain arbitrarily complex data structures, enabling new types of composable application development due to the zero-knowledge and private nature of data disclosure.

6 zkSNARKs as a service (zkSaaS)

Zero-knowledge applications in production pose new challenges for resource constrained devices. Mobile and browser based devices may not possess the compute power necessary to run these applications in a timely manner. In the academic literature, there have been several proposals from distributed computation [21] to new proof systems [2] to improve on the state of the art for these environments. Therefore, it's paramount that the exists infrastructure for offloading these computationally expensive jobs to a "cloud"-like environment.

Tangle aims to provide zkSNARKs as a service – otherwise described as proof generation as a service – for this very reason, to provide application developers with the ability to outsource a key component of their application's operations to a privacy preserving service. Leveraging key learnings from Webb's own development of zero-knowledge applications in the browser environment, it's extremely compelling from a UX perspective to be able to outsource proof generation to a privacy-preserving infrastructure. This eliminates a core challenge for developers, reducing the important process of interacting with zero-knowledge applications to simplified APIs that are as common to work with as any cloud based API service. These APIs can then be standardized to work seamlessly across the next thousand zero-knowledge applications that deploy to production.

Proof generation using MPC, discussed in the collaborative setting in [13], fits naturally into a blockchain environment. Tangle's validator set presents the perfect environment for mocking a "cloud" environment for outsourced proof generation. New participants can join the computation and existing ones can leave, while earning rewards throughout their participation. Recent research shows that zero-knowledge [8] and vanilla SNARK proof generation [12] have massive parallelization benefits when distributed across hundreds of nodes. Tangle aims to fit both on the privacy-preserving side as well as the non-private side to provide a service offering that eliminates friction for zero-knowledge and general SNARK application developers.

6.1 Targeted proof systems

- Groth16 [9]
- PLONK [7]
- Nova [11]
- Halo2 [3]
- Stark [1]

7 Trusted setups as a service (TaaS)

A core piece of any zero-knowledge application's deployment is the trusted setup. The trusted setup is a single event that is run to prepare a zero-knowledge application for production and requires a certain level of care to prepare. Often, projects will execute their trusted setup over months with hundreds of participants, where the only basic need is to generate trusted parameters for their application's operations. We envision a world with thousands of zero-knowledge applications and thousands of deployed circuits in production. In this world, completing a trusted setup should be quick and minimize the the efforts needed by a team. We envision a world where a single developer can deploy a zero-knowledge application to production and do so without organizing a trusted setup themselves.

Trusted setups have for the last many years been executed through MPC protocols, and Tangle can provide this primitive similarly to its others. The goal being to reduce the friction for any part of a zero-knowledge application's deployment to production.

7.1 Future services

Towards the purpose of enabling new applications and reducing friction for operating and deploying production applications, there are a variety of future MPCs we plan to explore for Tangle. Primarily, one of the last pieces of friction not mentioned in the services above is *witness generation*. On resource constrained devices, this too can pose challenges.

- **Data storage and availability for privacy applications.** Network validators and Tangle relayers can opt-in to storing datasets for other private applications for the expressed purpose of helping clients with witness generations.
- **Private information retrieval as a service**. By storing the datasets for other private applications, validators and Tangle relayers can opt-in to providing additional privacy preserving services to aid in the witness generation for zero-knowledge proofs.
- **Threshold decryption as a service**. Encrypted mempools are key to reducing MEV in blockchain ecosystems albeit a highly complex problem. This too can become an opt-in privacy-preserving service provided by Tangle's validators.
- **Sequencing as a service**. Building blocks for L2s remains an active topic in today's blockchain landscape. Proposals for block building in SGX have gained popularity because they enable privacy-preserving methods for ordering transactions in a block, preventing toxic MEV, and more. As Tangle grows its MPC offering, MPC could become a core tool used to achieve this goal.
- **Randomness beacons** A randomness beacon is a service that provides publicly verifiable, unbiased, and unpredictable random values at fixed intervals. It is designed to be used as a public utility, similar to how NTP provides timing information. The NIST Randomness Beacon, for example, generates full-entropy bit-strings and posts them in blocks of 512 bits every 60 seconds. Each value is sequence-numbered, time-stamped, and signed, and includes the hash of the previous value to chain the sequence of values together. The beacon is intended for various applications, such as selecting test and control groups for clinical trials, assigning court cases to random judges, or providing entropy to digital lotteries.

8 Restaking

Tangle's restaking system is directly baked into the runtime of the Tangle blockchain. Tangle restaking is only available to active validators on Tangle. An active validator can create a restaking profile by restaking 50% of their locked and nominated stake. In this manner, nominators of any actively restaking validator will also earn rewards proportional to their fraction of the total nominated stake.
Tangle's restaking system is directly integrated into its MPC-as-a-service infrastructure. Validators restake directly on the set of roles available to them in the runtime. These roles are protocol specific for any of the MPC protocols listed above. Each role represents an eligible service. For example, a subset of validators can restake on executing the CGGMP threshold ECDSA protocol [4] implemented in a specific open-source repository. Two different repos implementing the same protocol will be represented by two different roles. Extending this more generally, a role effectively maps to a unique implementation of an MPC protocol.

8.1 Supported MPC protocols

The protocols you will may on Tangle are:

- t-ECDSA CGGMP
- t-BLS381
- t-Schnorr
- t-zkSaaS
- Trusted Setup MPC
- And more...

8.2 Restaking Profile Creation

In order to begin restaking as a validator, one must create a restaking profile. Creating a profile involves restaking available stake to a subset of roles. Profiles are unique to each restaker. For each profile p we denote the following variables to be used to describe the restaking system.

- `total_restake`(p) - The total amount of tokens restaked in a profile.
- `role_restake`(p, r) - The amount of tokens restaked in a profile p on role r.
- `roles`(p) - The list of roles for this profile and their restake amounts.
- `jobs`(p) - The list of active jobs that have been requested for any role in the profile.

Definition 1. *An* ***independent restaking profile*** p *is one in which the restake amounts are allocated independently to each selected role such that*

$$\sum_{r \in p} \texttt{role\_restake}(p, r) = \texttt{total\_restake(p)}$$

Definition 2. *An* ***shared restaking profile*** p *is one in which the restake amounts are allocated collectively to all selected roles such that.*

$$\texttt{role\_restake}(p, r) = \texttt{total\_restake}(p)$$

Definition 3. *An* ***active profile*** p *is a profile such that*

$$|\texttt{jobs}(p)| > 0$$

8.3 Restaking Profile Updating

Updating a restaking profile is a permitted action as long as a variety of constraints are met. A restaker may update their restaking profile if they want to switch profile types, to increase or decrease the restake allocated to various roles, or to add or remove roles from their profile. The entirety of updating a restaking profile boils down to whether a profile p is active or not. If p is not active, then any profile updates are permitted. If p is active then we apply the following constraints.

Definition 4. *For an active profile p, let $\boldsymbol{r}$ be the roles with an active service/job. Let p' be the updated profile. A **profile update** is valid as long as the following holds*

- *If p and p' are the same profile type*

$$\forall r \in \boldsymbol{r},\ \texttt{role\_restake}(p', r) \geq \texttt{role\_restake}(p, r) \tag{1}$$

- *If p is an **independent profile** and p' is a **shared profile***

$$\forall r \in \boldsymbol{r},\ \texttt{total\_restake}(p') \geq \sum_{r \in \boldsymbol{r}} \texttt{role\_restake}(p, r) \tag{2}$$

- *If p is a **shared profile** and p' is an **independent profile***

$$\forall r \in \boldsymbol{r},\ \texttt{role\_restake}(p', r) \geq \texttt{total\_restake}(p) \tag{3}$$

Updating a profile must always preserve the restake amounts of active roles. If switching profile types from independent to shared, the total restake amount of the shared profile must be at least the sum of all independent restake amounts from the existing independent profile. If switching profile types from a shared to an independent profile, the restake amount on each independent role must be at least as much as the total restake amount from the existing shared profile. Meaning, going from shared to independent will always increase total restake amount, while going from independent to shared must simply preserve at least as much as the total restake amount prior to the update.

8.4 Restaking rewards

A major goal of Tangle's restaking system is the maximization of restaked Tangle Network Tokens (TNT). To incentivize validators to opt-in to MPC service roles and create profiles, the network rewards validators with additional inflationary rewards simply by restaking their tokens. This inflationary reward is in addition to the rewards they earn as validators. Once validators are restaked on a variety of roles, they must perform the services and jobs requested and paid for by customers.

By opting in and restaking, the restaking validator is effectively agreeing to the onchain service agreement and slashing conditions that amongst other protocol specific misbehaviours requires them to complete any requested services' jobs. Failure to complete any service for which one has restaked on is the first and simplest slashing condition. On top of restaking inflation, a validator also earns service fee rewards proportional to their amount of restaked funds for the active service in question.

Definitions for functions follow. Let v be a validator.

- `validator_inflation`$(v, \mathbf{T})$ - The validator's inflationary reward over the time interval $\mathbf{T}$ for validation activities.
- `total_val_inflation`$(\mathbf{T})$ - The total inflationary rewards distributed to validators over the time interval $\mathbf{T}$.
- `restaking_inflation`$(v, \mathbf{T})$ - The validator's restaking reward over the time interval $\mathbf{T}$ for restaking activities. Note, this will be zero if the validator is not restaking any tokens.
- `total_restaking_inflation`$(\mathbf{T})$ - The total inflation distributed to restakers over the time interval $\mathbf{T}$.

8.4.1 Service/job fees

Abstracting the protocol lifecycle, a customer requests a set of parties $p \in P$ to perform a service S composed of a set of jobs $j \in S$. We define the following variables to help describe the reward mechanism.

- $\texttt{job\_to\_fee}(j)$ - The service fee for the job.

The service fee for the job is determined based upon the size of the job, the length of the job, and other metadata related to job completion and computational expenditure. This function and all others can be updated using a runtime upgrade to influence the pricing and reward mechanisms.

8.4.2 Proportionality

In a proof of stake system, a validator v's stake fraction f_{stake} scales proportionally to the rewards issued to v over a time interval $\mathbf{T}$.

$$f_{stake}(v) \propto \frac{\texttt{validator\_inflation}(v, \mathbf{T})}{\texttt{total\_val\_inflation}(\mathbf{T})}$$

A restaker's rewards must scale proportionally to a variety of factors, namely, the amount of tokens restaked, the # of jobs completed, and the types of roles restaked on. The restaking inflation mechanism should adapt to the demand of the service mechanism as a whole, meaning that if a role has relatively few active jobs through a time interval $\mathbf{T}$ it should receive a relatively small proportion of the restaking inflation rewards. If $f_{restake}$ represents validator v's fraction of total restake, then the fraction of restaking rewards should follow similarly.

$$f_{restake}(v) \propto \frac{\texttt{restaking\_inflation}(v, \mathbf{T})}{\texttt{total\_restaking\_inflation}(\mathbf{T})}$$

Within the restaking inflation rewards, the per restaker rewards should scale proportionally to the amount of tokens restaked on that role versus other restakers on that same role. If the customer base demands a service from a certain subset of restakers, those restakers should earn more of the inflation relative to other restakers not participating in as many services or active jobs.

8.4.3 Target Restaking Rate

Similar to the target or ideal staking rate of a Substrate chain, Tangle implements a similar target rate for its restaking system. This rate is half of the ideal staking rate, or 25% of all tokens.

8.4.4 Reward function

In order to capture all information at our disposal we define

- $\texttt{job\_role\_distribution}(r, \mathbf{T})$ - The fraction of jobs with role r over the time interval $\mathbf{T}$.
- $\texttt{job\_restaker\_role\_distribution}(v, r, \mathbf{T})$ - The fraction of jobs with role r completed by validator v.
- $\texttt{restaking\_inflation}(\mathbf{T})$ - The annual percent inflation for restakers.

- $\texttt{total\_supply}(t)$ - The total supply of the TNT token at time t.

The reward function $\mathbf{R}$ for restakers over the time interval $\mathbf{T}$ is divided in half and distributed to two parts. The first part contextualizes the amount of work a validator has done. They are rewarded based on the fraction of total jobs they've participated in and completed. Therefore, the more active and trustworthy restaking validators are rewarded more than others. The second part of the reward is distributed proportionally to the restaking distribution. These two parts both allow us to reward active restakers but also restakers that haven't been selected for many jobs or any. This is done so we still continue to incentivize restaking at any cost.

We define some helper variables to fit $\mathbf{R}$.

$$\begin{aligned}\texttt{payout}(\mathbf{T}) &= \texttt{restaking\_inflation}(\mathbf{T}) * \texttt{total\_supply}(t)\\ \texttt{dist}(v, r, \mathbf{T}) &= \texttt{job\_role\_distribution}(r, \mathbf{T}) * \texttt{job\_restaker\_role\_distribution}(v, r, \mathbf{T})\end{aligned}$$

We now define the reward function $\mathbf{R}$.

Definition 5. *The reward function $\boldsymbol{R}$ for a validator v is defined as*

$$\boldsymbol{R}(v, \boldsymbol{T}) = \boldsymbol{\texttt{payout}}(\boldsymbol{T}) * \left(\sum_r \alpha_r \boldsymbol{\texttt{dist}}(v, r, \boldsymbol{T}) + (1 - \sum_r \alpha_r) f_{restake}(v)\right)$$

Theorem 8.1. *$\boldsymbol{R}(\boldsymbol{T}) = \boldsymbol{\texttt{payout}}(\boldsymbol{T})$*

Proof.

$$\begin{aligned}\mathbf{R}(\mathbf{T}) &= \sum_v \mathbf{R}(v, \mathbf{T})\\ &= \frac{\texttt{payout}(\mathbf{T})}{2} \sum_v \left(\sum_r \texttt{dist}(v, r, \mathbf{T}) + f_{restake}(v)\right)\\ &= \frac{\texttt{payout}(\mathbf{T})}{2} \left(\sum_r \sum_v \texttt{dist}(v, r, \mathbf{T}) + \sum_v f_{restake}(v)\right)\\ &= \frac{\texttt{payout}(\mathbf{T})}{2} \left(\sum_r \sum_v \texttt{dist}(v, r, \mathbf{T}) + 1\right)\\ &= \frac{\texttt{payout}(\mathbf{T})}{2} \left(1 + 1\right)\\ &= \texttt{payout}(\mathbf{T})\end{aligned}$$

□

9 Interoperability

At the heart of the Tangle Network is an unwavering dedication to blockchain interoperability. This section delineates our strategy and progression path toward realizing fluid cross-chain interactions, spanning from the bridging of assets to the provision of advanced cross-chain communication avenues. Cross-chain communication and asset transfer stand as the cornerstones of our initial interoperability strategies.

- **Privacy-Enabled Bridging:** Privacy-enabled Bridges have been core to the creation of Tangle, being the main application motivating the entire infrastructure. A proof of concept example is Hubble Bridge. Private bridges facilitate the transfer of assets between distinct chains in a privacy-preserved manner, empowering users with the ability to selectively disclose identifying information about their financial history.
- **zkBridges:** zkBridges such as Succinct's zk consensus bridge are pivotal to our inter-operability endeavors. Conceptualized as the principal conduits for asset movements and cross-chain dialogues, these bridges capitalize on cutting-edge cryptographic techniques and protocols., and guarantee efficiency, security, and adaptability in their operations.
- **IBC Pallets:** The infusion of IBC (Inter-Blockchain Communication) Pallets lays the groundwork for pioneering inter-chain dialogue and asset transference modalities.
- **XCM:** The forthcoming integration of Cross-Consensus Message (XCM) is set to supercharge our capabilities in cross-chain exchanges, paving the way for intricate and multifaceted interactions across chains.
- **Additional EVM Bridge Initiative:** This avant-garde initiative, details of which are closely guarded, is angled toward the establishment of a formidable infrastructure for interfacing with EVM-aligned chains. Collaborative endeavors are in the pipeline, with an active evaluation of potential grant recipients to actualize this visionary project.

10 Technical Specification

The Tangle Network presents an innovative solution for the implementation and governance of cross-chain Zero-Knowledge (ZK) applications as well as normal cross-chain applications. By utilizing the powerful and flexible Substrate blockchain framework, the Tangle Network serves as the foundational infrastructure to usher in a new age of privacy-centric and governance-decentralized applications.
The network's unique proposition lies at the intersection of cross-chain interoperability, compatibility with Ethereum Virtual Machine (EVM) tools, sophisticated governance mechanisms, and the realm of ZK applications. The Tangle Network integrates these distinct components seamlessly, resulting in a synergistic ecosystem that harnesses the strengths of each element.

10.1 Key Features

- **Built on Substrate:** The Tangle Network capitalizes on the advanced blockchain framework of Substrate, recognized for its versatility, scalability, and state-of-the-art features. This strategic selection certifies that our platform stays at the vanguard of rapidity, security, and scalability, acting as a dependable pillar for the Tangle Network. The modular design of Substrate facilitates smooth interaction and interoperability with other blockchain networks.
- **Advanced Governance:** The Tangle Network incorporates a pioneering governance model underpinned by a Distributed Key Generation (DKG) protocol. This protocol functions as a security mechanism for the network's cross-chain applications, validating bridge updates with crypto-economically protected threshold signatures. New DKGs will be added to interoperate with new signature schemes and further harden the security of Tangle.

- **MPC as a Service:** The Tangle Network natively supports a variety of multi-party computation primitives that aid in the development of new applications, especially zero-knowledge applications. These services benefit the Tangle community by positioning Tangle as a core piece of infrastructure for any zero-knowledge application across any ecosystem.

- **Privacy-Enhancing ZK Applications:** The Tangle Network prioritizes privacy by providing a platform for Zero-Knowledge (ZK) applications. These applications furnish users with privacy-enhancing functionalities, allowing them to transact, communicate, and interact securely while preserving the robustness and immutability of blockchain technology.

- **Cross-chain Functionality:** The Tangle Network transcends conventional chain limits supporting both IBC, XCM, zero-knowledge consensus based bridges, as well as the primitives for privacy-preserving bridges. The aggregation of these technologies connects Tangle to multiple ecosystems.

- **EVM Functionality:** The Ethereum Virtual Machine (EVM) is a critical component in the functionality of the Tangle Network, serving as a conduit for compatibility and interoperability with Ethereum-based tools and applications. Developers can seamlessly construct decentralized applications (DApps), generate Non-Fungible Tokens (NFTs), and utilize ERC20 tokens across diverse networks as they would on any other EVM.

- **Forkless upgrades:** Tangle is ready to integrate new technologies as soon as they are battle tested through Substrate's novel forkless runtime upgrades. This enables Tangle to rapidly innovate on both interoperability, scalability, and zero-knowledge application development.

10.1.1 Pallets

Tangle supports a myriad of core, native logic. This logic is defined in software modules called pallets. Many of the pallets used in Tangle are public goods of the Substrate blockchain framework and others are custom for the development of Tangle's unique MPC infrastructure. For the most up-to-date configuration of pallet's in Tangle's runtime, refer to the runtime module [18]. A non-exhaustive list of the most relevant pallets follows.

- **pallet-evm:** This pallet allows the execution of Ethereum smart contracts and transactions. It provides a sandboxed environment to run the EVM bytecode.

- **pallet-ethereum:** This pallet emulates Ethereum's state transition functions and transaction receipt logic.

- **pallet-evm-chain-id:** This pallet provides a chain ID, which is crucial for executing certain types of transactions such as those involving the EIP-712 typed signature hash.

- **pallet-dynamic-fee**: Adjusts transaction fees dynamically based on the state of the blockchain, helping to balance resource usage and revenue generation.

- **pallet-base-fee**: Implements a fixed base fee for transactions, providing a consistent minimal cost for operations on the network.

- **pallet-pallet-eth2-light-client**:Enables Ethereum 2.0 light client functionalities within the Substrate-based chain, facilitating cross-chain interactions with Ethereum networks.

- **pallet-randomness-collective-flip**: Provides a basic on-chain randomness beacon that's used for various decentralized operations such as lottery and elections.
- **pallet-balances**: Manages token balances and account liquidity, enabling token transfers and accounting within the network.
- **pallet-transaction-payment**: Handles the logic for transaction payments including fee deduction and refunding.
- **pallet-authorship**: Attributes block authorship, ensuring that block rewards and transaction fees are distributed to the appropriate block author.
- **pallet-babe**: Implements the BABE consensus algorithm for block production.
- **pallet-grandpa**: Implements the GRANDPA finality gadget, which allows for asynchronous block finality.
- **pallet-sudo**: Provides a single account (the "Sudo key") with superuser permissions capable of executing any operation on the network.
- **pallet-indices**: Manages shortened account IDs to allow for more human-friendly addressing.
- **pallet-democracy**: Enables on-chain governance mechanisms like referenda and public proposals.
- **pallet-collective**: Implements council-based governance features including motions and voting.
- **pallet-vesting**: Manages vesting schedules for tokens, allowing for time-based token releases.
- **pallet-elections-phragmen**: Provides an implementation of the Phragmén election algorithm for choosing network representatives.
- **pallet-election-provider-multi-phase**: Offers a two-phase election model for improved efficiency and security.
- **pallet-staking**: Manages the staking mechanism, enabling nominated proof-of-stake operations.
- **pallet-session**: Manages session keys and validators, handling the rotation of authorities for each new session.
- **pallet-session-historical**: Keeps historical session records, useful for features that need to access past sessions.
- **pallet-treasury**: Manages a decentralized treasury, funding community proposals and initiatives.
- **pallet-bounties**: Enables users to propose and fund bounties for tasks or improvements within the network.
- **pallet-child-bounties**: Extends the bounties pallet to allow for the creation of sub-bounties or child bounties.

- **pallet-bags-list**: Implements a "bag" storage optimization for efficient on-chain storage of large datasets.
- **pallet-nomination-pools**: Manages pools of nominees for network validators.
- **pallet-scheduler**: Allows for scheduling future tasks or events on the blockchain.
- **pallet-preimage**: Manages the storage and revelation of preimages for governance proposals.
- **pallet-offences**: Handles reporting and punishment for misbehaving validators.
- **pallet-transaction-pause**: Provides a mechanism to temporarily pause specific transactions.
- **pallet-im-online**: Verifies the online status of validators, enhancing network security.
- **pallet-identity**: Manages on-chain identities, providing a way to link multiple accounts and off-chain information.
- **pallet-utility**: Offers various utility functions like batch transactions and proxy capabilities.

10.2 Consensus and Finality

Substrate distinguishes between block authoring and block finality through two different mechanisms. Tangle uses BABE (Blind Assignment for Blockchain Extension) to reach consensus on block authors. BABE selects validators according to the Nominated Proof of Stake system as well as a verifiable random function (VRF). Each validator is assigned a weight for an epoch. This epoch is broken up into slots and the validator evaluates its VRF at each slot. For each slot that the validator's VRF output is below its weight, it is allowed to author a block.
For finality, Tangle uses GRANDPA. GRANDPA provides block finalization. It has a known weighted authority set like BABE. However, GRANDPA does not author blocks. It just listens to gossip about blocks that have been produced by block authoring nodes. GRANDPA validators vote on chains, not blocks. GRANDPA validators vote on a block that they consider best and their votes are applied transitively to all previous blocks. After two-thirds of the GRANDPA authorities have voted for a particular block, it is considered final. [5]

10.3 Validator Selection: Nominated Proof of Stake (NPoS)

The Tangle Network, like most Substrate-based chains including Polkadot [20], employs a variant of Proof of Stake (PoS) known as Nominated Proof of Stake (NPoS) [15]. This mechanism is used to select validators and issue rewards.

10.3.1 Overview

In contrast to traditional PoS systems, nPoS introduces the role of nominators, alongside validators. Validators handle the responsibilities of maintaining the network and producing new blocks, while nominators support one or more validators with their stake. This additional layer of stake backing enhances the security and decentralization of the network. The nPoS system is designed to be highly inclusive, striving to increase the number of validators, thereby mitigating the risk of centralization. Furthermore, nPoS works to ensure that validators are both competent and well-behaved.

10.3.2 Validators and Nominators

Within the nPoS model, validators are nodes that hold the responsibility of block production and network maintenance. The election of validators is based on the total stake backing them, which comprises their own stake and that of their nominators.
Nominators, meanwhile, are stakeholders who back one or more validators for election. They delegate their tokens to these validators, sharing in the rewards and risks of the validators they back.

10.3.3 Staking and Slashing

The process of staking involves locking tokens via the staking pallet, which enables participation in the network as a validator or nominator. The likelihood of a validator being selected for block production is directly proportional to the number of tokens staked on their behalf, including both their own stake and that of their nominators.
A key component of the nominated Proof-of-Stake system is the slashing mechanism. If validators act maliciously or fail to fulfil their roles— for example, by being offline or failing to validate correctly— they stand to lose a portion of their stake. This loss, known as slashing, can also impact nominators who back a slashed validator.

10.4 Balances and Accounts

A fundamental component of many Substrate-based blockchains, including the Tangle Network, is the Balances pallet. This module manages fungible assets, predominantly native tokens of a blockchain, overseeing everything from their creation to transfer. It enables token transfers, reserves tokens for specific functions, and applies rules related to minimum balance.

10.4.1 Accounts and Address Mapping in Frontier

Every participant in a blockchain is represented by an account, uniquely distinguished by a public key. Within the context of Substrate chains and Ethereum, these accounts manifest differently. Substrate's flexible account system accommodates multiple types of accounts, such as those using Ed25519, Sr25519, or ECDSA public keys. In contrast, Ethereum uses only ECDSA based accounts.
Frontier, as an Ethereum compatibility layer for Substrate, bridges this disparity through an address mapping mechanism. This mapping allows Ethereum addresses to correspond with their respective Substrate addresses, facilitating the interaction between the two distinct account systems. When a user or developer interacts with the Ethereum environment on a Frontier-enabled Substrate chain, this mapping ensures that operations targeting an Ethereum address are correctly relayed to its associated Substrate account in the runtime.

Through Frontier's address mapping, Substrate chains achieve near-complete Ethereum compatibility, enabling Ethereum DApps, tools, and other functionalities to operate on the Substrate environment seamlessly, while still retaining the native capabilities and features of Substrate.

11 TNT Token Details and Economics

11.1 Token Utility

The Tangle Network Token (TNT) serves multiple functions within the network. It acts as a utility token facilitating gas metering for smart contract execution, protocol security, on-chain governance, and network transactions. Its utilities include:

- Gas Metering: Supporting the gas metering of smart contract execution.
- Protocol Security: Incentivizing validators and powering the mechanics around the creation of a decentralized node infrastructure.
- On-chain Governance: Facilitating the on-chain governance mechanism, including proposing referenda, electing council members, and voting.
- Network Transactions: Paying for transaction fees on the network.

11.2 Token Distribution

Tangle Network has tailored its genesis allocation to meet its unique needs and goals, taking inspiration from successful networks as a benchmark.

11.2.1 Vesting Schedules

> **Claims Window:** Genesis participants will have 1 year to claim their distribution, **the deadline is April 10, 2025.** Otherwise, the amount is sent to the Tangle Network on-chain treasury.

Vesting schedules in Tangle Network are designed to promote long-term commitment and ensure a phased distribution of tokens. The network adopts a structured vesting strategy with distinct categories:

A-Vesting: This category is characterized by a vesting period of 2 years, with a 12-month cliff. This means that no tokens are released in the first year. After completing the first year (the cliff period), the tokens allocated for that year become immediately available in full. The remainder of the allocation is then distributed monthly in equal 1/12 increments over the second year, facilitating a gradual release of tokens. This approach aligns with the policy of Immediate Vesting Post-Cliff with Retroactive Accumulation.

B-Vesting: This vesting category is tailored for airdrop participants, featuring a 2-year vesting period with a notably short cliff of just 1 month. A predefined percentage of tokens becomes immediately available at the start. Subsequent to the cliff period, the remaining tokens are distributed on a monthly basis, ensuring a consistent flow of tokens into circulation. This strategy also follows the Immediate Vesting Post-Cliff with Retroactive Accumulation policy, aiming to reward early supporters while promoting long-term holding.

11.2.2 Detailed Allocation Overview

The Tangle Network's allocation model is designed to support our foundational structures, incentivize community participation, and ensure long-term sustainability and success:

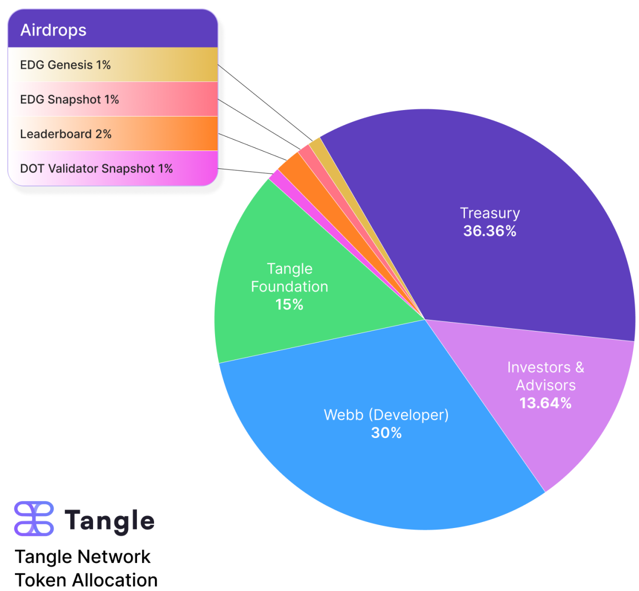

Figure 3: Allocation Pie Chart

- **Contributors** allocation supports the core teams, core-team investors, and advisors essential for the network's development and strategic direction.
- **Airdrops** are aimed at rewarding and incentivizing validators, early supporters, and participants, fostering a strong and engaged community from the outset.
- **Governance-Managed** funds are earmarked for community decision-making, future development, network success programs, liquidity provisions, and partnerships critical for growth.

Table 1: Allocation Table: Categories and Totals

Allocation Category	**Entity Name**	**Allocated Share (%)**	**Total Tokens Allocated**
Contributors	Webb (Developer)	28.56500%	28,565,000.00
Contributors	Investors	13.64000%	13,640,000.00
Contributors	Indiv. Contributors	1.43500%	1,435,000.00
Contributors Total		43.64000%	43,640,000.00
Governance-Managed	On-chain Treasury	36.36000%	36,360,000.00
Governance-Managed	Foundation	15.00000%	15,000,000.00
Governance-Managed Total		51.36000%	51,360,000.00
Airdrop Pool	Leaderboard Participants	2.00000%	2,000,000.00
Airdrop Pool	DOT Validators Snapshot	1.00000%	1,000,000.00
Airdrop Pool	EDG Genesis Participants	1.00000%	1,000,000.00
Airdrop Pool	EDG 2023 Snapshot	1.00000%	1,000,000.00
Airdrop Pools Subtotal		5.00000%	5,000,000.00
Total Supply		100.00000%	100,000,000.00

Table 2: Allocation Table: Vesting Schedule Details

Entity Name	**Vesting Plan**	**Cliff**	**Vesting**	**Imm. Liq.**	**Initial Liquid**	**Cliff-Release**	**Monthly Rate**
Webb (Developer)	A-Vesting	12	24	0%	0.00	14,282,500.00	2,380,416.67
Investors	A-Vesting	12	24	0%	0.00	6,820,000.00	1,136,666.67
Indiv. Contributors	A-Vesting	12	24	0%	0.00	717,500.00	119,583.33
On-chain Treasury	n/a	n/a	n/a	100%	n/a	n/a	n/a
Foundation	A-Vesting	12	24	5%	750,000.00	593,750.00	619,565.22
Leaderboard Participants	B-Vesting	1	24	5%	100,000.00	79,166.67	82,608.70
DOT Validators Snapshot	B-Vesting	1	24	5%	50,000.00	39,583.33	41,304.35
EDG Genesis Participants	B-Vesting	1	24	5%	50,000.00	39,583.33	41,304.35
EDG 2023 Snapshot	B-Vesting	1	24	5%	50,000.00	39,583.33	41,304.35

11.2.3 Release Schedule

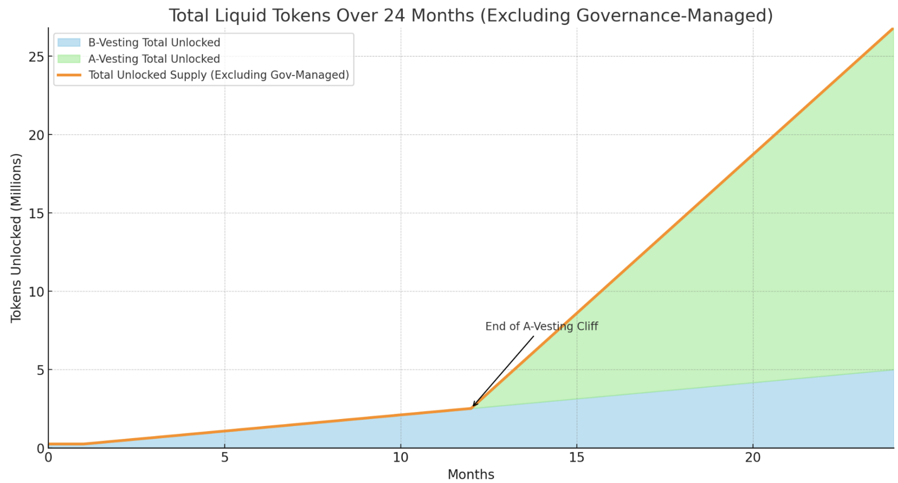

Figure 4: Liquid Tokens Over Time

11.2.4 Token Allocation and Vesting Schedule Formulas

This section outlines the formulas used to calculate various aspects of our token allocation and vesting schedules.

Initial Liquid Tokens
$\text{Initial Liquid Tokens} = \text{Total Tokens Allocated} \times \text{Immediate Liquidity Percentage}$
Calculates the number of tokens that are immediately liquid and available at launch, based on the total tokens allocated to an entity and the percentage designated as immediately liquid.

Cliff-Release Tokens (for entities with a retroactive vesting cliff)
$\text{Cliff-Release Tokens} = \text{Total Tokens Allocated} \times \frac{\text{Cliff Duration}}{\text{Total Vesting Period}}$
For allocations with a retroactive vesting cliff, this calculates the number of tokens released at the end of the cliff period, based on the total allocation and the proportion of the vesting period represented by the cliff.

Monthly Vesting Rate (for entities with post-cliff monthly vesting)
$\text{Monthly Vesting Rate} = \frac{\text{Total Tokens Allocated} - \text{Initial Liquid Tokens} - \text{Cliff-Release Tokens}}{\text{Vesting Period} - \text{Cliff Duration}}$
Determines the monthly rate at which tokens vest after the cliff period, considering the total tokens allocated minus any initially liquid tokens and tokens released at the cliff, divided by the remaining months of the vesting period.

Special Considerations
For entities without a vesting plan (e.g., Treasury, Foundation), the entire allocation is considered

liquid at launch, though it is only utilized through governance and so not 'liquid' in the traditional tokenomic sense.

11.3 Definitions

1. **Allocation Category**: A grouping used to categorize the distribution of tokens or shares within a project or organization, typically indicating the purpose or recipient of the allocation.
2. **Entity Name**: The name of the individual or organization receiving the allocation of tokens or shares.
3. **Allocated Share**: The percentage of the total token supply allocated to a specific entity or category.
4. **Vesting Plan**: A structured timeline outlining how allocated tokens or shares become available to the recipient over a period, usually to incentivize long-term commitment or performance.
5. **Cliff (Months)**: The initial period after which a portion of the allocated tokens or shares becomes accessible to the recipient, often used as a safeguard against early departures or underperformance.
6. **Vesting Period (Months)**: The total duration over which allocated tokens or shares gradually become available to the recipient according to the vesting schedule.
7. **Immediate Liquidity**: The percentage of allocated tokens or shares that are immediately accessible or liquid upon allocation, without being subject to vesting restrictions.
8. **Initial Liquid Tokens**: The number of tokens or shares initially available for immediate use or transfer upon allocation.
9. **Cliff-Release Tokens**: The number of tokens or shares released after the cliff period, becoming accessible to the recipient according to the vesting schedule.
10. **Monthly Vesting Rate**: The rate at which tokens or shares vest on a monthly basis after the cliff period, determining the pace of distribution to the recipient.
11. **Total Tokens Allocated**: The overall sum of tokens or shares allocated to a specific entity or category, representing the total amount of ownership or participation assigned.
12. **Contributors**: Individuals or entities actively involved in contributing to the project's development, growth, or success.
13. **Governance-Managed**: Tokens allocated for governance purposes and managed by a designated entity or organization within the project, typically used for decision-making or protocol governance.
14. **Airdrops**: Distribution of tokens to a specific group of recipients, often as a promotional or community-building activity, without requiring direct financial investment.

15. **Leaderboard Participants**: Participants who engage with the project's leaderboard, often in competitions or challenges, and receive tokens as rewards or incentives.

16. **DOT Validators Snapshot**: Participants included in a specific snapshot of DOT (Polkadot) validators and rewarded with tokens accordingly.

17. **EDG Genesis Participants**: Participants involved in the project's Sept 2017 genesis event.

18. **EDG 2023 Snapshot**: Participants included in a snapshot of block 18070680 (July-31-2023 06:28:12 AM +-5 UTC) and eligible for token rewards based on their inclusion in the snapshot.

19. **Total Supply**: The overall quantity of tokens or shares in existence within the project or organization, representing the maximum potential ownership or participation.

12 Inflation and Staking Rewards

12.1 Overview

Tangle Network utilizes a Nominated Proof of Stake (NPoS) system to secure its network and incentivize participation. The creation (minting) of new Tangle Network Tokens (TNT) serves as the primary mechanism for rewarding validators and nominators, which in turn introduces inflation into the system. This section outlines the key aspects of how rewards are distributed and how inflation is managed within Tangle Network.

12.2 NPoS Payments and Inflation

- **Purpose**: Rewards are distributed to validators and nominators for their roles in block production and network security.
- **Inflation**: The minting of new TNT for rewards is the main source of inflation within Tangle Network.
- **Exclusions**: This overview **does not** account for penalties (slashings), rewards for reporting misconduct, or transaction fee rewards, which are covered separately.

12.3 Inflation Model Simplified

- **Staking Rate**: (x)
  Represents the proportion of total TNT supply that is staked in the NPoS system.
- **Ideal Staking Rate**: (χ_{ideal})
  The target staking rate Tangle Network aims to achieve for optimal security and liquidity balance.

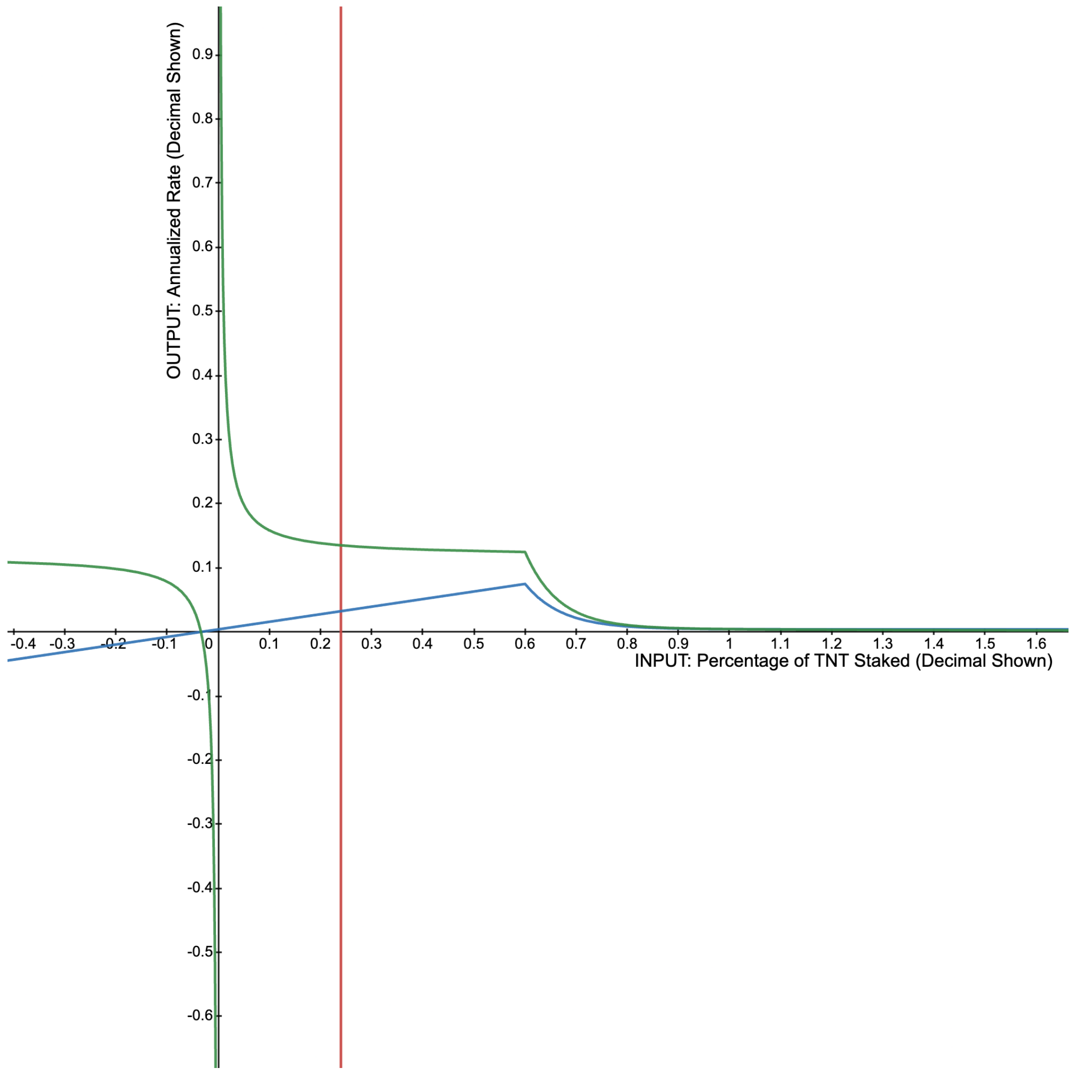

Figure 5: Inflation Model

- **Yearly Interest Rate**: ($i(x)$)
  The rate at which rewards are paid out relative to the amount staked, adjusted based on the staking rate to incentivize desired staking levels.

Key Concepts:

- **Incentives**: The system adjusts rewards to encourage a staking rate close to χ_{ideal}, reducing rewards as staking exceeds this target to prevent liquidity issues.
- **Inflation Rate** (I): Calculated based on several factors, including rewards for NPoS participation, treasury funding, penalties, and transaction fees. The goal is to balance inflation with network security and operational needs.
- **Adjustable Parameters**: The model includes variables like the ideal interest rate (i_{ideal}) and inflation limits that can be tuned to manage the network's economic dynamics effectively.

12.4 Reward Distribution Mechanism

Validators and nominators receive rewards for their contributions to block production and network security, with rewards calculated based on several factors including the total points earned for various actions within the network. Rewards are allocated based on a point system, where different network contributions earn different points. The total payout is then distributed proportionally to the points earned by each participant.

12.5 Inflation Control and Staking Incentives

The inflation model is designed to encourage a balanced staking rate by adjusting rewards based on the current staking rate relative to the ideal target. The ideal staking rate may be adjusted to account for factors such as network growth and operational needs, in order to maintain network security and efficiency.
While the underlying mechanics of the inflation model are complex[6], the essence is to incentivize behaviors that secure the network and ensure its smooth operation, balancing between rewarding participation and controlling inflation. The community and governance processes play a crucial role in adjusting parameters within the inflation model to respond to evolving network needs and conditions. This simplified overview aims to provide a clearer understanding of how Tangle Network manages inflation and rewards within its NPoS system, making the information accessible to a broader audience without diminishing the intricacies of the underlying mechanisms.

13 Network Launch and Genesis

13.1 Launch Date

The Tangle Network testnet will go live September 20th, 2023, and the Webb-coordinated Mainnet launch on April 10, 2024.

13.2 Initial Network Setup

The Network will initially launch with 10 validators. As security and stability are achieved, Webb intends to regularly scale this using the governance proposal system. The initial distribution of validators is intended to produce multiple types of decentralization, including geographic, technological and more. These nodes may also fulfill roles relating to the Webb Protocol Relayer system [17].
The genesis configuration, in the form of a 'chainspec.rs', will be shared through the Tangle Network github repository

13.3 Network Participation

1. **Stay Updated**: Ensure you're up-to-date with the latest announcements and updates. Subscribe to our official channels, including our website, newsletter, and social media platforms.

2. **Set Up a Wallet**: To interact with our chain, you'll need a compatible wallet. If you already have a substrate-based wallet, ensure it's updated to the latest version. We recommend Polkadot Apps for a secure experience.

3. **Acquire Tokens**: Our chain's native token will be essential for various network activities. Users can obtain these tokens through our initial distribution events, grants, on-chain actions, or exchanges.

4. **Connect to the Network**: Once the network is live, connect your wallet to our chain using the provided RPC endpoints.

5. **Deploy and Interact with Smart Contracts**: Developers can deploy their Ethereum smart contracts on our chain, taking advantage of the EVM compatibility. Use popular Ethereum tools and frameworks for a seamless development experience.

6. **Staking and Validation**: To secure our network, users can participate as validators or nominators. Detailed guides on the rewards mechanism, staking and setting up a validator node are available on our documentation.

7. **Community Engagement**: Join our community forums, discussions, and governance proposals. Your feedback and participation will shape the network's future direction and growth. These channels will be shared on our documentation and blog.

8. **Developer Grants and Hackathons**: Developers are encouraged to build on our platform. We'll be rolling out grant programs and organizing hackathons to foster innovation and growth in our ecosystem.

14 Roadmap

1. **Research & Whitepaper Release**: Publish comprehensive research on EVM compatibility and its importance. Release the initial whitepaper detailing the project's vision, technical specifications, and goals.
2. **Prototype Development**: Develop an initial version of the EVM module for Substrate. Test the prototype with basic Ethereum smart contracts.
3. **Testnet Launch**: Launch a public testnet with EVM compatibility. Invite developers to test and provide feedback.
4. **Integration of Ethereum Tools**: Ensure compatibility with popular Ethereum tools like Truffle, Remix, and MetaMask. Develop plugins or extensions if necessary.
5. **Smart Contract Deployment**: Enable the deployment of existing Ethereum smart contracts on the testnet. Test and optimize for gas usage and contract execution speed.
6. **Interoperability Testing**: Test cross-chain functionalities, ensuring seamless interaction between Ethereum and the Substrate chain. Implement and test bridges or relays for asset transfers.
7. **Mainnet Launch**: Launch the mainnet with EVM compatibility. Ensure robust security measures and optimizations are in place.
8. **Community and Developer Engagement**: Organize hackathons, workshops, and developer bootcamps. Provide grants or incentives for dApp development on the new chain.
9. **Governance Implementation**: Implement on-chain governance mechanisms. Engage the community in decision-making processes.
10. **Performance Optimization**: Continuously monitor and optimize the chain's performance. Implement layer-2 scaling solutions if necessary.
11. **Partnerships and Integrations**: Form strategic partnerships with other projects in the Polkadot/Substrate and Ethereum ecosystems. Integrate with DeFi projects, wallets, and other platforms.
12. **Upgrades and Feature Releases**: Regularly release updates to improve EVM compatibility, security, and performance. Introduce new features based on community feedback and emerging industry trends.
13. **Security Audits**: Conduct regular security audits of the EVM module and other critical components. Address any vulnerabilities or issues identified.
14. **Expansion to Other Ecosystems**: Explore and develop compatibility with other blockchain ecosystems beyond Ethereum. Test and deploy bridges to other chains.
15. **End-User Education**: This is an ongoing task. Develop comprehensive documentation, tutorials, and guides. Educate the community about the benefits and use-cases of the EVM-compatible substrate chain.

15 Governance

15.1 Overview of Governance

Decentralized blockchain networks like Tangle Network rely on on-chain governance for continuous evolution and protocol upgrades. Governance involves key roles played by the council and token holders:

- The council is elected by token holders and is responsible for proposing referenda, vetoing harmful initiatives, and representing passive token holders.
- Token holders actively engage by voting on referenda, suggesting changes, and electing council members.

Tangle Network employs adaptive quorum biasing, adjusting the proposal passing threshold based on turnout. This allows for network evolution without hard forks, ensuring uninterrupted services.
Governance is further enriched by public referenda, accessible to any TNT token holder willing to provide a bond. Proposals can be initiated by any token holder, and others can endorse these by seconding them with tokens equivalent to the original bond.

15.1.1 Governance Interfaces

Tangle Network provides two interfaces for managing voting, discussions, proposals, and running for office, Polkadot JS ('Apps').

16 Community

Our community forms the backbone of Tangle Network, consisting of a dynamic mix of developers, privacy researchers, decentralized app (dApp) users, bridge users, and token holders. Due to the pseudonymous nature of blockchain spaces, it's hard to quantify the exact count. However, we have a thriving presence online, with 2000 members in our Discord and 3400 followers on our Twitter.
The community members assume various roles within our ecosystem. This includes, but is not limited to, technology advocates, validators, data relayers, governance participants, and open-source contributors. Our codebase is publicly accessible on Github, which encourages transparency and open-source contributions.

16.1 Communication Channels

We maintain an active presence across multiple platforms to foster transparency and community engagement. Our official communication channels include Twitter, Telegram, Discord, and Github.

16.2 Support and Resources

Our extensive documentation serves as a primary source of information and support for our community members. Should they need further assistance, they are always welcome to reach out via our Discord or Telegram channels.

17 About the Team

Tangle Network is spearheaded by Drew Stone, a notable figure in the blockchain domain with a rich history of leading tech-centric initiatives. His commitment to blockchain privacy is encapsulated in his founding of the Webb Protocol [17], a cutting-edge cross-chain zero-knowledge messaging layer. This protocol is designed to augment privacy across blockchains, thereby facilitating secure financial, identity, and social applications in a multi-chain landscape.

17.1 Drew Stone's Background

Drew Stone's foundational work in the blockchain community is evident in his substantial contributions before the establishment of Webb Protocol. As co-founder at Commonwealth Labs, he played a pivotal role in the development of Edgeware, marking its position as the inaugural mainnet in the Polkadot ecosystem. Further bolstering his credentials, Drew holds a degree in Mathematics from the University of Pennsylvania, seamlessly combining his academic prowess with practical blockchain development expertise.

18 Conclusion

18.1 Summary

The Tangle Network introduces an innovative platform to support cross-chain Zero-Knowledge (ZK) applications and enhance privacy in the blockchain ecosystem. Built on the robust Substrate framework, Tangle Network aims to address key challenges around privacy and interoperability. The network goes beyond just enabling ZK applications by also providing MPC-as-a-Service (MaaS), making advanced cryptographic operations more accessible for application developers.
Some of the main technical achievements of Tangle Network include:

- Cross-chain functionality and EVM compatibility via Substrate Frontier.
- Advanced cryptographic techniques such as zero-knowledge proofs, multi-party computation, and distributed key generation.
- A unique offering of MPC-as-a-Service, including Signing as a Service and Proof Generation as a Service.
- Specialized use-cases like interoperable shielded pools, social and identity bridges, and on-chain oracles.

With these features, Tangle Network offers unique benefits to users, developers, and validators. Collaborations within the blockchain community are fundamental to Tangle Network's progress.

18.2 Future Prospects

In the short term, the roadmap focuses on mainnet launch, collaborations, and community growth. This includes not only forming partnerships but also extending the capabilities of MPC-as-a-Service for a wider range of cryptographic applications.

The long-term vision sees Tangle Network as a core infrastructure for enabling privacy-first and interoperable blockchain solutions. New services like MPC-as-a-Service are stepping stones toward achieving this vision, simplifying the development and deployment of advanced cryptographic applications.

Ongoing R&D will focus on optimizations like improved transaction speed, enhanced cryptographic techniques, and additional privacy layers. The network also aims to offer more customizable and versatile services, adapting to the needs of an evolving blockchain ecosystem.

Expanding the community and integrating with other protocols will be crucial. This includes fostering environments where developers can easily implement zero-knowledge proofs and other advanced cryptographic techniques.

Lastly, education around zero-knowledge technology and decentralized governance will be pivotal as interest in privacy and decentralization continues to grow. The network is well-positioned at the forefront of the privacy-focused blockchain movement, aiming to address challenges like governance attacks proactively.

With a robust platform and clear roadmap, Tangle Network is positioned at the forefront of the privacy-focused blockchain movement.

References

[1] Eli Ben-Sasson et al. "Scalable zero knowledge with no trusted setup". In: *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III 39*. Springer. 2019, pp. 701–732.

[2] Jonathan Bootle et al. "Gemini: Elastic SNARKs for diverse environments". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2022, pp. 427–457.

[3] Sean Bowe, Jack Grigg, and Daira Hopwood. "Recursive proof composition without a trusted setup". In: *Cryptology ePrint Archive* (2019).

[4] Ran Canetti et al. "UC non-interactive, proactive, threshold ECDSA with identifiable aborts". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 2020, pp. 1769–1787.

[5] *Consensus — Substrate Docs — docs.substrate.io*. https://docs.substrate.io/learn/consensus/. [Accessed 13-09-2023].

[6] Web3 Foundation. *Token Economics*. URL: https://research.web3.foundation/Polkadot/overview/token-economics.

[7] Ariel Gabizon, Zachary J Williamson, and Oana Ciobotaru. "Plonk: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge". In: *Cryptology ePrint Archive* (2019).

[8] Sanjam Garg et al. "zkSaaS: Zero-Knowledge SNARKs as a Service". In: *Cryptology ePrint Archive* (2023).

[9] Jens Groth. "On the size of pairing-based non-interactive arguments". In: *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II 35*. Springer. 2016, pp. 305–326.

[10] Kobi Gurkan, Koh Wei Jie, and Barry Whitehat. "Community proposal: Semaphore: Zero-knowledge signaling on ethereum". In: *Accessed: Jul* 1 (2020), p. 2021.

[11] Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla. "Nova: Recursive zero-knowledge arguments from folding schemes". In: *Annual International Cryptology Conference*. Springer. 2022, pp. 359–388.

[12] Tianyi Liu et al. "Pianist: Scalable zkRollups via Fully Distributed Zero-Knowledge Proofs". In: *Cryptology ePrint Archive* (2023).

[13] Alex Ozdemir and Dan Boneh. "Experimenting with Collaborative {zk-SNARKs}:{Zero-Knowledge} Proofs for Distributed Secrets". In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, pp. 4291–4308.

[14] Torben Pryds Pedersen. "Non-interactive and information-theoretic secure verifiable secret sharing". In: *Annual international cryptology conference*. Springer. 1991, pp. 129–140.

[15] *Polkadot Consensus · Polkadot Wiki — wiki.polkadot.network*. https://wiki.polkadot.network/docs/learn-consensus#nominated-proof-of-stake. [Accessed 13-09-2023].

[16] Adi Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[17] Drew Stone. *Webb Protocol: A cross-chain private application and governance protocol*. 2023. URL: https://eprint.iacr.org/2023/260.pdf.

[18] *tangle/standalone/runtime/src/lib.rs at main · webb-tools/tangle — github.com*. https://github.com/webb-tools/tangle/blob/main/standalone/runtime/src/lib.rs. [Accessed 13-09-2023].

[19] EigenLayer Team. *EigenLayer: The Restaking Collective*. Accessed: 01-15-2024.

[20] Gavin Wood. "Polkadot: Vision for a heterogeneous multi-chain framework". In: *White Paper* (2016).

[21] Howard Wu et al. "{DIZK}: A distributed zero knowledge proof system". In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018, pp. 675–692.