Tangle Network: An MPC-as-a-service blockchain infrastructure for powering cross-chain and zero-knowledge applications.

Drew Stone, Thom Ivy

hello@webb.tools

September 19, 2023

Abstract

This paper introduces the Tangle Network, a platform designed to support cross-chain Zero-Knowledge (ZK) applications. Built on the Substrate blockchain framework, the Tangle Network provides a platform for privacy-enhancing and governance-decentralized applications, incorporating cross-chain functionality, EVM compatibility, advanced governance systems, and ZK applications into a unified ecosystem. The network enables interaction, data exchange, and operation of ZK applications across different blockchain networks, facilitated by the Ethereum Virtual Machine (EVM) [17] on Substrate. An innovative governance model, based on Distributed Key Generation (DKG) protocol, ensures the validity of updates within the network's cross-chain Anchor zkApps. The paper explores the technical specifications, potential applications, and the theoretical and practical benefits of this system.

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 Webb's Zero-knowledge Messaging Infrastructure

Tangle's roots are grounded in the development of the Webb Protocol [15] having been born and developed by the Webb team. The Webb Protocol is a system for building and governing cross-chain applications that can support shared anonymity set functionality across a set of identical bridged systems on compatible blockchains. The protocol addresses privacy and scalability concerns that have become increasingly prevalent in the domain of decentralized applications. It does this through a shared zero-knowledge messaging layer denoted the Anchor System.

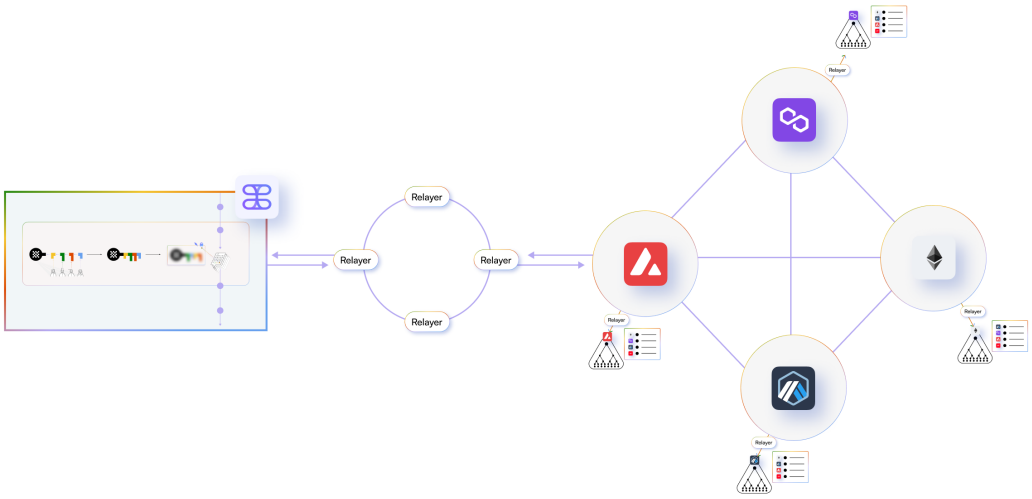

Figure 1: Overview of the Webb Protocol Ecosystem

Tangle natively supports the infrastructure and primitives necessary for building Anchor System instances for the purposes of developing new cross-chain zero-knowledge applications. Using a hybrid threshold and trustless light-client validation protocol, updates over this messaging layer are trust-minimized and cost efficient. This design permits threshold-signed messages to be validated while enforcing message integrity and existence from a connected blockchain. It is in this context that the Tangle Network pushes the frontier of possible zero-knowledge application development.

3.1.1 Anchor System

The Anchor System is a specification for a cross-chain stateful applications built over a graph-like framework. Nodes are referred to as anchors and edges represent the connections between neighboring anchor states. Each anchor has an on-chain Merkle tree and an edge list that manages and updates the connected metadata. The system relies on an external protocol to ensure liveness and safety, which are paramount to guaranteeing continuous and correct updates of all anchors in the system.

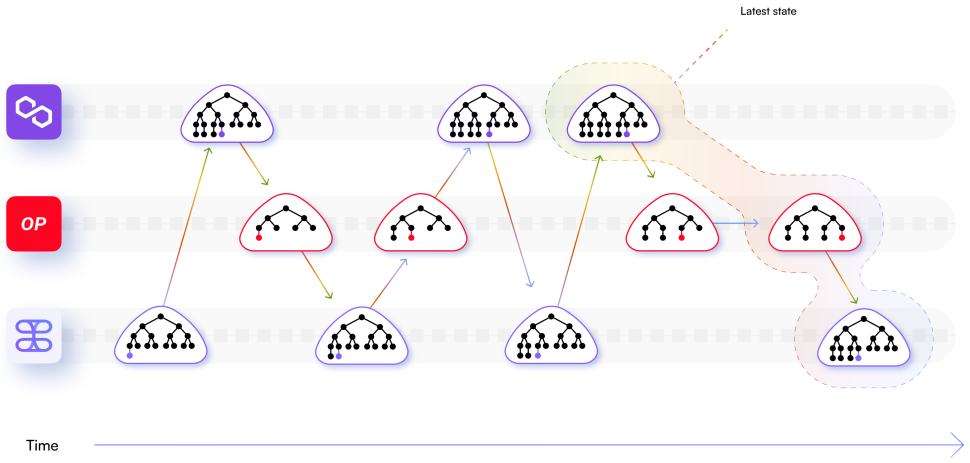

Figure 2: Overview of the Anchor System and State

The Tangle network supports Anchor System instances at the base layer. New cross-chain zero-knowledge applications need only propose through governance to be integrated and operated by Tangle's infrastructure. The Tangle DKG's validate and sign payloads for transmitting cross-chain zero-knowledge messages and Tangle's relayer network transmits these payloads to their destinations. Together the DKG and relayer network preserve the liveness and safety as per the conditions outlined in the Webb Protocol whitepaper. We describe in detail the types of applications enabled by these primitives in later sections.

3.2 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.

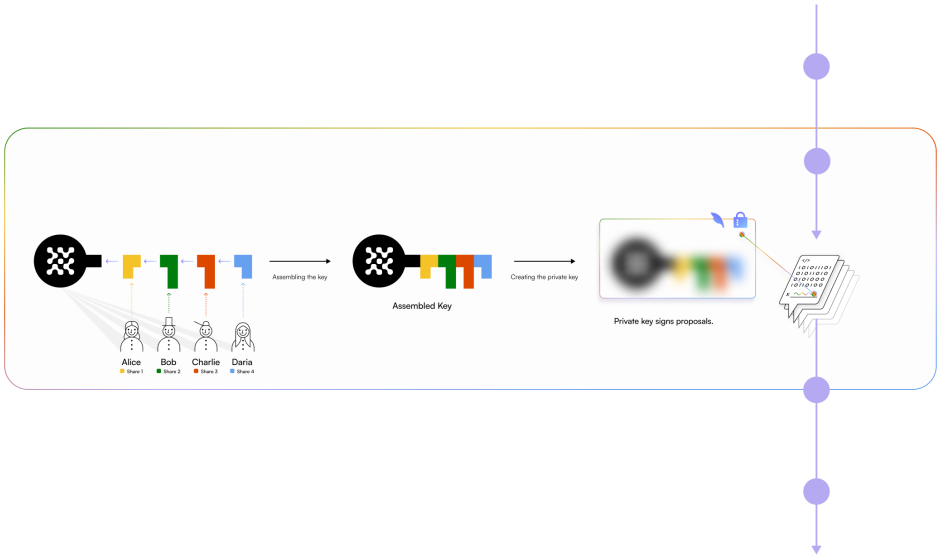

Figure 3: An example of the Threshold Signature Scheme offered in Tangle Network.

MPC protocols rely heavily on certain primitives such as secret sharing [14] 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.

3.3 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 [12]. 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.

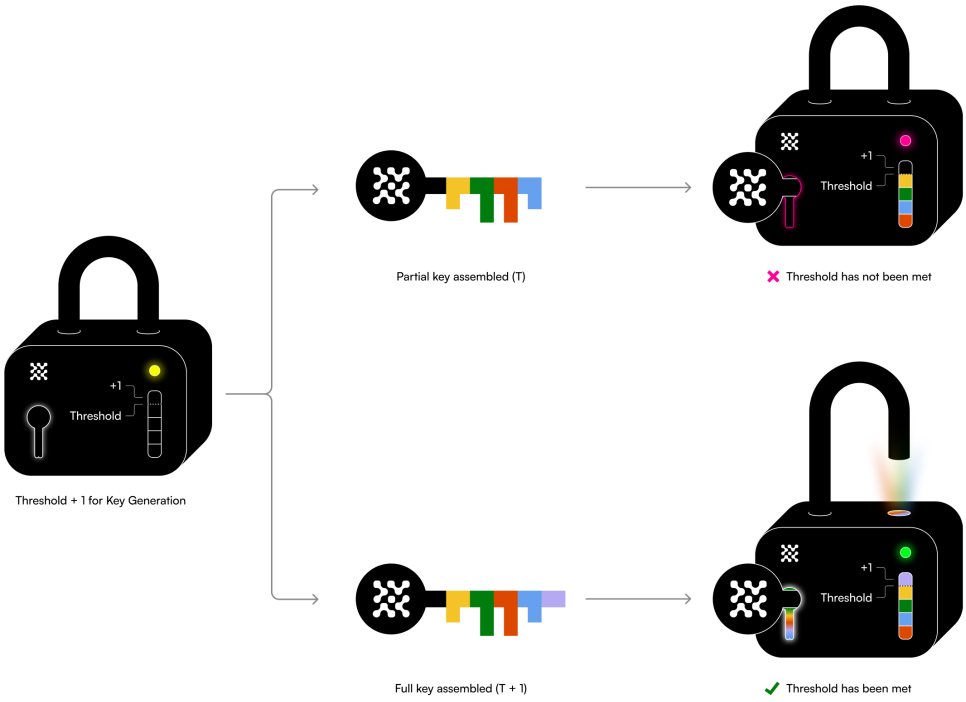

Figure 4: Distributed Key Generation analogized with keys broken into multiple shards.

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.

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.
The protocol's validator set runs these protocols on demand to provide services that target cryptographic and especially 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 initial network focuses on the following MPC primitives:

- Signing as a service
- Proof generation as a service
- Trusted Setup generation as a service

5 Signing as a service (SIGNaaS)

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 cmoplex 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. 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, 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 [8] 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.

5.4 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 [19] 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 [11], 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 [6] and vanilla SNARK proof generation [10] 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.

5.4.1 Targeted proof systems

- Groth16 [7]
- PLONK [5]
- Nova [9]
- Halo2 [3]
- Stark [1]

5.5 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.

5.6 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.

6 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.

- **Private Bridge:** Private 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.

7 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.

7.1 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.

7.2 Technical Specifics of DKG in the Tangle Network

The implementation of DKG in the Tangle Network involves several specific mechanisms:

7.2.1 Authority Selection

The authority selection system for DKG authorities uses a reputation mechanism for selecting the best set of authorities to participate in the key generation and signing protocols. For a keygen threshold of n and a signing threshold of t, the top-n authorities on-chain by reputation are selected. Out of these n keygen authorities, t+1 are selected for signing. The keygen set remains fixed over the course of the session, whereas the signing set can change amidst misbehaviours in the signing protocol.

7.2.2 Jailing Authorities

Authorities implicated in verified and reported misconduct will be temporarily suspended or "jailed" for a specific number of sessions, preventing their inclusion in the authority selection process. This punitive measure against malicious behaviour suspends the authority for a predetermined period.

7.2.3 Key Rotation

To maintain a high level of security, the Tangle Network necessitates the periodic rotation of shared private signing keys. At the start of a new session, the new authorities are selected, and the next authorities generate a new group key pair on-chain, denoted next_dkg_public_key. The current authorities, if it is time to refresh, begin to sign the next_dkg_public_key with their key, the dkg_public_key. The signature from the active key pair of the next key pair is posted on-chain, marking a successful key rotation.

7.2.4 Misbehaviour Reporting & Reputation

Misbehaviour within the Tangle Network is identified and reported through an oracle-based approach, utilizing a threshold voting-based approach for identification. The DKG protocol has identifiable aborts, enabling the detection of misbehaving parties during the protocol's execution. If a threshold number of parties report the same misbehaviour, the offending party's reputation is reduced according to the function:

$$reputation(o) = \alpha * reputation(o)$$

Conversely, when a good action occurs, such as a successful key rotation or signing and submission of a proposal, the reputation of the respective party increases according to the function:

$$reputation(o) = \alpha * reputation(o) + 1,000,000,000$$

7.2.5 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 [16]. A non-exhaustive list of the most relevant pallets follows.

- **pallet-dkg-metadata:** This pallet tracks information about the DKG state, handling sub-protocols such as refresh protocol and misbehaviour and reputation protocol.
- **pallet-dkg-proposals:** This pallet maintains the valid proposers and the first layer of the governance system. The valid proposers is a superset of the current DKG authorities.
- **pallet-dkg-proposal-handler:** This pallet implements the ProposalHandlerTrait and accepts proposals through this handler system.
- **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-aura**: Implements the Aura consensus algorithm for block production, usually used in proof-of-authority networks.
- **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.

7.3 Consensus and Finality

Substrate distinguishes between block authoring and block finality through two different mechanisms. Tangle uses the Proof of Authority consensus system Aura to reach consensus on block authors. Aura provides a slot-based block authoring mechanism. In Aura a known set of authorities take turns producing blocks.
Tangle may switch at launch to a more robust consensus protocol such as BABE. BABE provides slot-based block authoring with a known set of validators and is typically used in proof-of-stake blockchains. Unlike Aura, slot assignment is based on the evaluation of 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. [4]

7.4 Validator Selection: Nominated Proof of Stake (NPoS)

The Tangle Network, like most Substrate-based chains including Polkadot [18], employs a variant of Proof of Stake (PoS) known as Nominated Proof of Stake (NPoS) [13]. This mechanism is used to select validators and issue rewards.

7.4.1 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.

7.4.2 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.

7.4.3 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.

7.5 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.

7.5.1 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.

8 TNT Token Details and Economics

8.1 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.

8.2 Token Supply and Distribution

The initial supply of TNT is set at 10 million. Details about the token allocation and any vesting or lock-up periods can be found in the Tangle Genesis Allocation Details.

8.3 Staking and Rewards

Tangle Network employs a staking mechanism built upon the Substrate framework. This mechanism is designed to incentivize validators and nominators to act in the best interest of the network. The staking rewards are dynamically set, based on an inflationary model aiming to achieve a targeted staking rate. The specifics of penalties for misbehavior and the manner in which rewards are divided between validators and nominators are under consideration.

8.4 Monetary Policy

The token supply may change over time, following an algorithmic inflation model. The rate of inflation is dynamic and changes according to the network's targeted staking rate. While Tangle Network is considering implementing a burn mechanism, the specifics remain to be determined.

8.5 Modeling

Details about token economics modeling will be included in future versions of this whitepaper to provide a comprehensive understanding of how the token's utility is expected to drive demand.

8.6 Compliance

Updates concerning compliance with legal regulations will be provided closer to the mainnet launch, and this whitepaper will be updated accordingly.

9 Network Launch and Genesis

9.1 Launch Date

The Tangle Network testnet will go live September 20th, 2023, and the Webb-coordinated Mainnet launch is currently planned for Q1 of 2024. We will announce formal dates through our official channels at Twitter and the Webb Blog

9.2 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.
The genesis configuration, in the form of a 'chainspec.rs', will be shared through the Tangle Network github repository

9.3 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.

10 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.

11 Governance

11.1 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.

11.1.1 Governance Interfaces

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

12 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.

12.1 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.

12.2 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.

13 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, 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.

13.1 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.

14 Conclusion

14.1 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.

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

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

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

[7] 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.

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

[9] 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.

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

[11] 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.

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

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

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

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

[16] *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].

[17] Gavin Wood et al. "Ethereum: A secure decentralised generalised transaction ledger". In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.

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

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