IoTeX 2.0 – DePIN for Everyone!

Version 1.1

The IoTeX Team

17 July 2024

Abstract

Decentralized physical infrastructure network (DePIN) is currently one of the hottest narratives in Web3 and represents a major paradigm shift that could fundamentally change how physical infrastructure networks are built, operated and managed in the near future. Due to the lack of funds and technical competence, emerging DePIN startups are facing significant challenges to bring their ideas to the market in a timely manner. In this whitepaper, we present IoTeX 2.0, a transformative step in the evolution of the IoTeX network, aiming to address the aforementioned challenges and help the DePIN community realize the ultimate vision of "DePIN for Everyone!".

IoTeX 2.0 contains the following core innovations:

- A new tokenomic design that explores the utility of IOTX tokens in the modular DePIN infrastructure extensively;
- A modular DePIN infrastructure that allows DePIN startups to build their applications on top of a community-owned, decentralized infrastructure;
- A modular security pool (MSP) that provides a unified trusted layer for DePIN infrastructure modules via restaking;
- A decentralized multi-prover network called W3bstream that allows DePIN builders to leverage different validity proof approaches to realize DePIN verification;
- A unified identity system called ioID that manages and secures machine-to-machine and machine-to-person relationships on-chain/off-chain in DePIN applications;
- A universal embedded SDK called ioConnect that empowers device abstraction and facilitate interaction of smart devices in DePIN applications;

- A chain SDK called ioDDK that allows DePIN projects to provision self-sovereign application chains and inherit the security of IoTeX L1 simultaneously.

Contents

Chapter 1

DePIN Today

IoTeX was founded in 2017 to empower people to own and control their smart devices, as well as the data and value their devices produce, by connecting the Internet of Things (IoT) with blockchain. Our founding thesis was that the orchestration of billions of smart devices using decentralized blockchains would resolve major issues with the existing Internet of Things, such as trust, security, and interoperability, as well as enable a new paradigm for user-owned device networks to flourish. Over the past 6 years, we have pioneered the synthesis of the real world and blockchains, exploring and building out several core use cases:

- **Micropayments (2017-2018)**: Use blockchain as a global, digital settlement layer to facilitate automated, cheap payments between devices, machines, and people. Blockchains serve as a unifying layer for previously non-interoperable devices to communicate and transact.
- **Provenance and supply-chain (2018-2020)**: Utilize blockchain as a trustless accounting and ownership ledger, enabling provenance for smart devices and decentralized supply-chain use cases (e.g., Pebble Tracker [1,2]). Blockchain collects data from trusted devices to verify real world activities as well as triggers new events and workflows.

- **Data ownership and privacy (2020-2021)**: Use blockchain as a decentralized identity layer to enable people to own and control their devices and data (e.g., Ucam [3,6]), incorporating advanced cryptography such as end-to-end encryption, multi-party computation, and confidential computing. Decentralized privacy solutions developed in partnership with major enterprises like Arm [7,8].

- **DePIN (2021-present)**: Use blockchain as the foundation for **De**centralized **P**hysical **I**nfrastructure **N**etworks (DePIN), a new model for capital formation and human coordination that allows people to contribute to and build equity in real world infrastructure networks. The data and services that DePINs produce may also serve as inputs to other use case categories, namely Artificial Intelligence (AI) and Real World Assets (RWA).

The original IoTeX whitepaper [5] published in 2017 showcased our vision for a secure, scalable, multi-purposed and decentralized L1 that incorporates privacy-preserving technologies and device-oriented middleware to connect the physical and digital worlds. Over the years, we have realized many of the ambitious goals we set out to accomplish in our original whitepaper:

- The IoTeX Mainnet has processed $\sim$120 millions of transactions without any downtime or hacks;

- The first blockchain-compatible hardware devices (e.g., Ucam and Pebble Tracker) were designed and manufactured by IoTeX as out-of-the-box hardware developer kits for builders;

- A variety of smart devices from third parties have been integrated to the IoTeX platform, providing a fundamental understanding of how to connect the real world securely to blockchain;

- An entire ecosystem of DePIN projects has been launched on IoTeX that incorporates real world data from smart devices;

- A global community of network validators, developers, and users has been created that represents the lifeblood of the IoTeX Network.

But this is just a start. The blockchain landscape has grown exponentially since 2017 and we now have a deeper understanding of what is necessary for DePIN to reach mass adoption. In parallel with building our original IoTeX vision, the IoTeX coredev has been busy researching and designing new innovations to bring DePIN to the next level, such as zero-knowledge proofs, off-chain scaling, self-sovereign identity for devices, and public goods that drive the entire DePIN sector forward.The IoTeX 2.0 vision we're introducing outlines our three-year plan to expand the IoTeX Network. We aim to incorporate a new modular platform design, update our tokenomics, and more to meet the increasing demands of builders in the DePIN space and beyond. With this updated vision, we can finally realize our ultimate goal of empowering "**DePIN for Everyone!**".

1.1 Why DePIN Is Important

Before we dive into IoTeX 2.0 and our vision for the future of DePIN, we would like to start by sharing what DePIN is and why you should care. Today, many of our world's most important industries and public utilities, such as telecom, energy, and compute, are monopolies and oligopolies that are owned and controlled by centralized corporations and governments. These trillion-dollar industries are designed with extremely high barriers to entry, both financial and logistical; for example, AT&T spends $24 billion annually and requires more than $160,000$ employees to run their telecom empire. Because of these massive barriers to entry, there are only a few providers for goods and services that everyday people can choose from. This means competition is limited, innovation is stifled, and consumers have to put up with subpar customer service and overly inflated prices because they donât have any other choice. As they provide services to millions of customers, corporate giants also stealthily extract sensitive and valuable data from people for their own profits. The issues that stem from this are even more

pronounced in emerging markets countries, further deepening the wealth gap and restricting opportunities for everyday people.

DePIN is a revolutionary concept that will change the status quo. DePINs that are built on open-source, decentralized blockchains can bring transparency, trust, and innovation to the physical infrastructure and public utilities that serve billions worldwide with low or no cost. But fixing today's world is only a fraction of DePIN's true potential. The real opportunity is not to simply patch over what's wrong with the current world, but to build a new world with utilities that are owned, operated, and utilized by everyday people. DePINs will enable anyone to contribute to and build equity in real world infrastructure networks, overcoming the aforementioned financial and logistical barriers to entry. By utilizing the novel capital formation methods popularized by Decentralized Finance (DeFi) to crowdsource network resources, DePINs can aggregate user-contributed hardware, manpower, and regional expertise to drive the buildout of new infrastructure networks and reward contributors with equity in the networks that they help create. Finally, DePINs can leverage immutable smart contracts on the blockchain to verify and coordinate the actions of contributors towards what is best for the network.

DePIN not only provides a path to improve our current world, but also offers an opportunity to design a better world. We are at the precipice of a new industrial revolution where decades-old infrastructure, such as fossil fuels and wired internet, will be replaced by innovative infrastructure, such as renewable energy and wireless. With DePIN, everyone can become a contributor to the modernization of our global infrastructure and receive their fair share of the trillions of dollars in value that this infrastructure represents. A new world by the people, for the people – that is the promise of DePIN. DePIN, is for everyone!

1.2 The DePIN Landscape

DePIN is a collective effort from hundreds of projects around the world all driving towards the decentralization and improvement of our physical infrastructure.

Although the term DePIN was created in 2023, the DePIN sector has been active for much longer with projects like IoTeX, Helium, and Filecoin serving as pioneers since 2017. Today, the DePIN landscape is diverse and consists of projects building DePIN-specific infrastructure as well as DePIN applications across several verticals. DePIN is now one of the most promising use cases for blockchains and can be subdivided into physical resource networks and digital resource networks, which are designated by the type of service a network provides. Physical resource networks produce non-fungible resources (i.e., the data/services from any devices are unique) that are more tangible in nature and generally rely on location-dependent hardware. On the other hand, digital resource networks produce marketplaces for fungible resources (i.e., 1GB of storage is 1GB of storage) that are more virtual in nature and rely on hardware that is location-agnostic. The DePIN sector also includes infrastructure and tooling that facilitate the category's growth and provide off-the-shelf capabilities for DePIN applications. A comprehensive DePIN landscape is shown in Figure 1.1.

1.3 The DePIN Tech Stack and Its Challenges

Regardless of whether a DePIN focuses on physical resources or digital resources, or what specific vertical they target, the need for an end-to-end tech stack that connects the real world to the blockchain world is necessary. Unlike blockchain use cases that facilitate the exchange of digital assets such as NFTs and financial assets such as stablecoins, DePINs must interface with real world smart devices that generate an incredible amount of data. Blockchain, as an immutable ledger, is a perfect foundation to document facts about what happened in the real world; however, before writing "proofs of real world activity" from devices to the blockchain permanently, a series of steps must be completed to verify the real world activity actually happened and the data is trustworthy. Devices must be registered on-chain, raw data must be collected, parsed, and stored, and computations over data must be performed in a verifiable fashion before any "proof of real world activity" can be settled to a blockchain. The reference architecture [9]

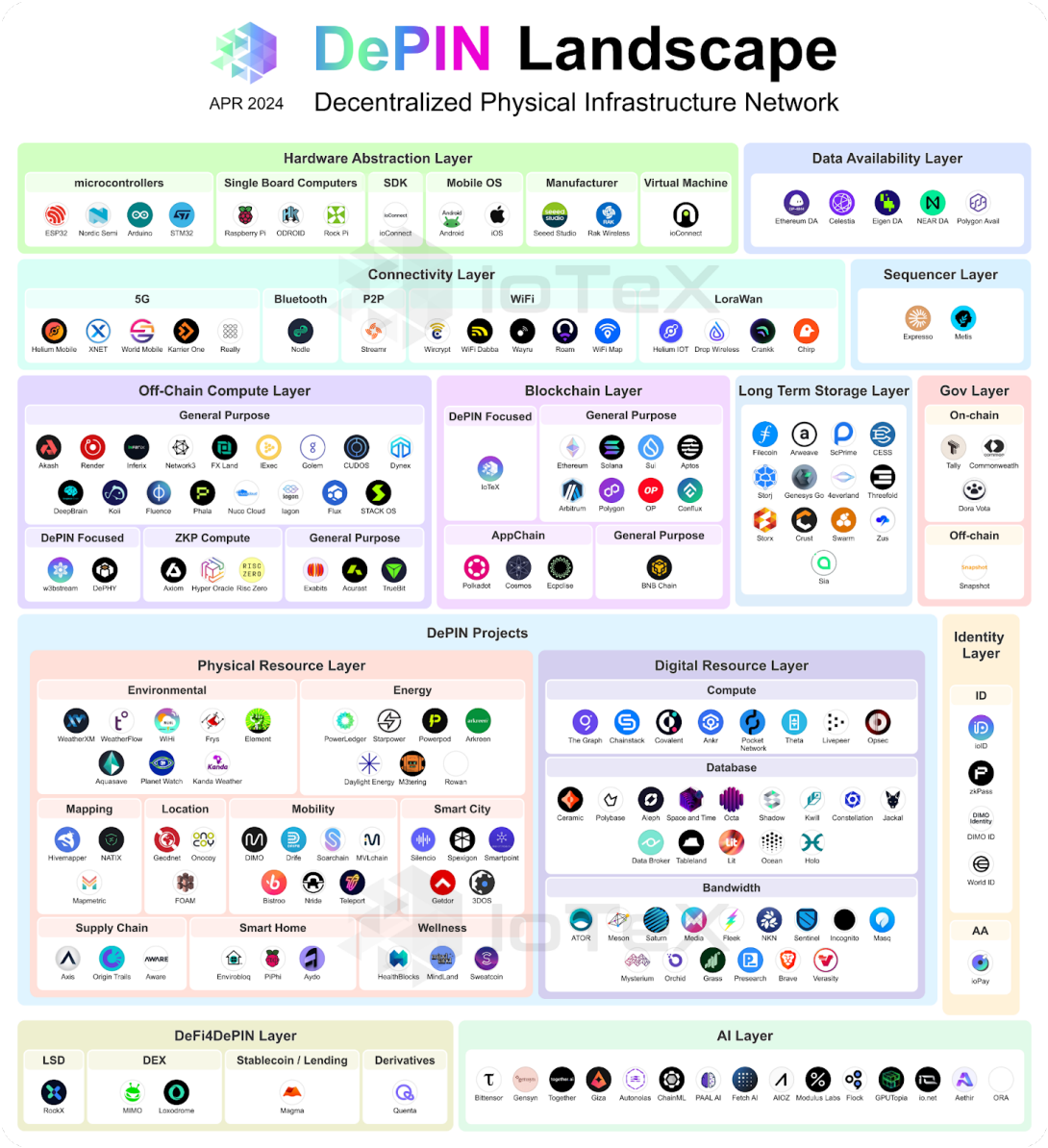

Figure 1.1: The DePIN Landscape

as shown in Figure 1.2 introduces nine essential layers for DePIN projects to consider.

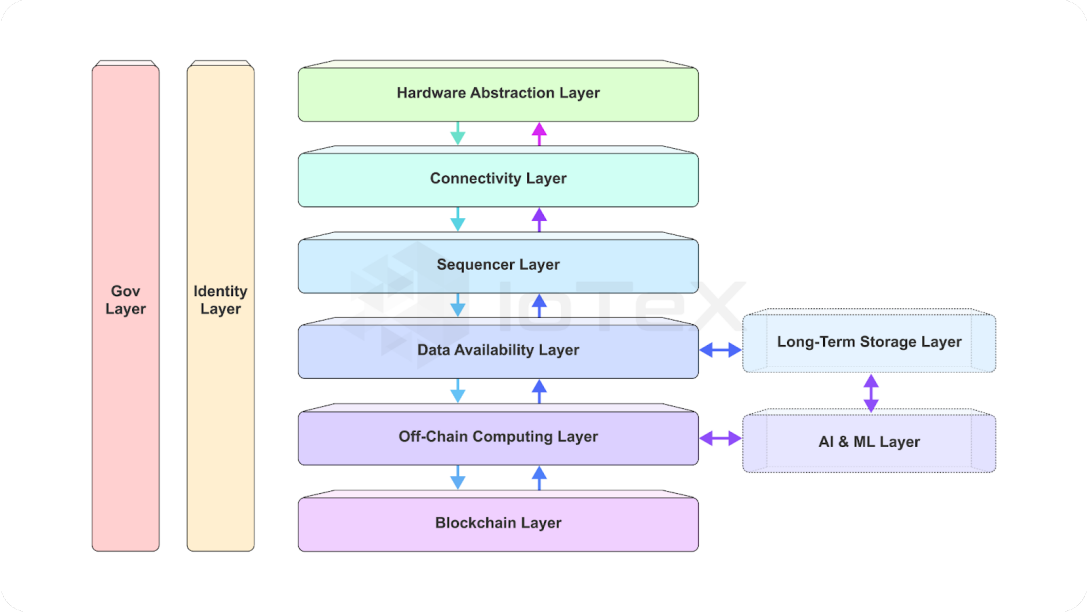

Figure 1.2: The DePIN Tech Stack

- **Hardware Abstraction Layer**: facilitates a wide range of smart devices, big or small, to securely connect with entities in the Connectivity Layer
- **Connectivity Layer**: reliably relays data produced by smart devices to the Sequencer Layer
- **Sequencer Layer**: orders data packets from smart devices before sending them to the Data Availability Layer
- **Data Availability Layer**: stores data for immediate use and security verification, allowing off-chain devices to access the information and generate insights from raw data
- **Long-Term Storage Layer**: archives raw data and insights for future use, which can be accessed by third parties via APIs for compliance, analytics, AI, and more

- **Off-Chain Computing Layer**: applies business logic to the data stored in the Data Availability Layer to generate insights and proofs related to real world activity
- **Blockchain Layer**: serves as the trust anchor for device identities and data, verifying the validity of off-chain computations and distributing token rewards to DePIN stakeholders
- **Identity Layer**: manages on-chain and/or off-chain identities for all involved entities (e.g., smart devices, users, servers, manufacturers, validators)
- **Governance Layer**: enforces network policies and procedures (e.g., incentives) in a decentralized fashion, typically through a community voting process.

The extensive layers of the DePIN tech stack can be overwhelming for a single team to develop in a monolithic fashion. This complexity creates a high barrier to entry for builders to experiment with innovative ideas in DePIN. In the past few years, well-funded projects have overcome these challenges by raising significant venture capital and developing their own monolithic tech stacks. However, for DePIN to truly flourish and reach every corner of the world (such as LATAM, Africa, and SouthEast Asia), the large tech stack and high tech complexity present additional challenges:

- **Launch Velocity**: the speed at which DePINs can reach a minimum threshold of supply to drive initial demand is limited due to hardware constraints and upfront capital expenditure requirements;
- **Demand-Side Growth**: DePINs struggle with building demand due to the long journey to bootstrap supply and difficulty in achieving parity with existing solutions for user experience, reliability, and cost;

- **Token Liquidity**: DePINs use token incentives to fuel network growth and fund infrastructure operations, but struggle with closing the flywheel and building on-chain liquidity;
- **Awareness**: DePINs often focus on specific industries, where the project's purpose and metrics for success are not always obvious, especially to those that are not already directly involved in the industry.

Due to these challenges, DePIN is still fairly nascent and has not yet surpassed DeFi and other crypto sectors in terms of market value and adoption. DeFi and DePIN are similar in many respects, most notably that they crowdsource resources from people (the "supply side") to create a product that other people desire and use (the "demand side"). However, the path to obtaining and maintaining supply and demand is vastly different between DeFi and DePIN. At a high level, DeFi supply and demand is easier to bootstrap but is fleeting while DePIN supply and demand is harder to bootstrap but is more capable of standing the test of time. Furthermore, DePINs often must aggregate a large supply of resources to create initial demand, unlike DeFi where a small amount of aggregated funds may have immediate demand. Comparing DePIN and DeFi side-by-side against the challenges noted above, we can see the following detailed distinctions as shown in Figure 1.3.

1.4 Our Philosophy for DePIN

We strongly believe that DePIN is for everyone: every builder, every contributor, and every user. This belief underlines that:

- Small teams and even solo developers should be able to build impactful DePIN products using best-in-class infrastructure.
- DePIN projects should be quickly iterated without high upfront costs to identify real innovation.

- Projects under DePIN should be composable both in terms of function (for instance, aggregating data from ring, car, phone for an individual) and region (such as Uber's city-by-city model).
- Network contributors providing value or utility to the network should have a low entry bar, and be financially rewarded in a stable, long-term way.
- Users should be able to enjoy equitable access to public, innovative utilities from these DePIN networks.

This belief is not merely wishful thinking. It can be practically translated into a technical design, known as IoTeX 2.0, as shown below.

Aspect	Tech Stack	Launch Velocity	Demand-side Growth	Token Liquidity	Sharing Network Growth
DeFi	Simple and digital-only: e.g., Solidity + JS mostly, easy to fork-to-launch	Fast: e.g., launch dApp globally; a few "miners" with large capital set up the supply-side quickly	Easy to attract users, esp. With incentives like yield farming, but those are usually short-lasting	Token liquidity is easy to acquire and a natural byproduct of a financial application	Metrics for success are clear e.g., TVL and easy to pull and display
DePIN	Complicated and touches the physical world: C/C++ + Golang/ Python/Rust + Solidity + JS + optional Swift, hard to fork	Slow: e.g., ship and deploy project-specific hardware, threshold-scale of supply at which the network can serve demand may be high	Slow to bootstrap, e.g., onboarding cellular plan customers, but can be more impactful over the long-term	Token liquidity is often difficult to achieve because founders and contributors have more hardware and Web2 experience than financial experience	Metrics for success are project-specific and must be pulled from physical devices
Challenges for DePIN	Challenge 1: DePIN projects are harder to build and require more capital to launch due to their hardware components. Exploration is slow and expensive.	Challenge 2: DePIN projects are slow to launch (establish the supply side) due to their hardware constraints, which can create a mismatch with crypto cycles.	Challenge 3: Crypto can provide an underwhelming UX, slowing demand-side adoption	Challenge 4: Token liquidity is particularly difficult to establish for DePINs that power network growth with token incentives	Challenge 5: DePIN teams must spend valuable time and effort building dashboards to display their project metrics
Partial Solutions	Launch projects in a centralized way to "test" the market and speed decision-making. The lack of decentralization and trustlessness may disappoint customers and investors.	Working with an existing Web2 partner, e.g., T-Mobile, to reach threshold-scale faster. Does not apply to innovative DePIN networks where a Web2 partner does not exist.	Using tokens to incentivize everyday people to adopt and use a DePIN, but most people are not crypto-native and don't understand tokens, wallets, etc.	DePIN teams can work with CEXes and market makers to attain token liquidity. This can be an expensive and lengthy process.	On-chain data can be somewhat easily pulled and displayed with tools like Dune. However, many DePINs are quite centralized and don't have much on-chain data to show.

Figure 1.3: A Comparison between DePIN and DeFi

Chapter 2

IoTeX 2.0

2.1 Introduction

IoTeX 2.0 defines the grand vision and roadmap of the IoTeX Network for the next several years, expanding on our mission to enable "DePIN for Everyone" and stemming from years of experience as a pioneer of the DePIN industry. Our goal is to not only address the technical and non-technical challenges that DePIN projects face today, but to realize the full potential of DePIN in the future by making IoTeX the largest DePIN ecosystem in the world. To achieve this, we are excited to present IoTeX 2.0, which combines new philosophy, technology, tokenomics, public goods, and initiatives to enable everyday people to contribute to DePINs and empower builders to truly bridge the real world to the blockchain world.

With IoTeX 2.0, the IoTeX Network will evolve from simply a L1 blockchain to an open DePIN infrastructure, Dapps, and L2s that will be anchored via the IOTX token. This will greatly increase the number and types of participants and contributors to the IoTeX Network to ultimately expand the reach of IoTeX and DePIN to new frontiers. DePIN should be for everyone, which is why IoTeX 2.0 prioritizes the inclusion of builders and users at every stage of the life cycle. Whether you are an established Dapp that wants to expand to your own L2

chain, or a traditional company seeking to implement a DePIN-based business model, or just a small team with a big idea, IoTeX 2.0 provides a complete suite of capabilities that are relevant for all DePIN builders.

Our core methodology is the modular DePIN infrastructure: DePIN projects can construct the tech stack that suits their specific stage and requirements by choosing from a menu of modular offerings. These offerings include in-house products built by IoTeX coredev and partner products from top projects. A primary advantage of the modular approach is enabling infrastructures builders to focus on functionalities they do best and collaborate to achieve the common goal. Our modular offerings incorporate cutting-edge technology such as off-chain scaling, zero-knowledge proofs, and artificial intelligence to bring unique innovations to the DePIN sector. These modules are built not only by IoTeX coredev but also by specialized infrastructure builders, using IoTeX to ensure their security and trust. This approach provides the largest DePIN teams with comprehensive solutions, while also offering smaller teams purpose-built solutions they can use to create new DePIN projects quickly and securely.

From an architectural perspective, IoTeX 2.0 emphasizes the following perspectives (see Figure 2.1):

- **Modular Security Pool (MSP)**: The basis for modularity is a unified, trusted layer, supported by IOTX and other mainstream assets, which we refer to as MSP. These are a set of smart contracts deployed on the IoTeX L1. Both the IoTeX L1 and MSP serve as the trust anchor and unchangeable ledger for all activities within the DePIN Infrastructure Modules (DIM) Layer and Dapp/L2 layers. Broadly speaking, the MSP allows the IoTeX L1 to lend its proof-of-stake security to DIMs that span various parts of the DePIN tech stack. DIM providers will stake IOTX and other mainstream assets to join the MSP. Furthermore, DIMs that obtain security and trust from the MSP will intermittently anchor their states to the IoTeX L1, opening up the possibility for dApp builders to innovate based on trusted real-world activity.

- **DePIN Infrastructure Modules (DIMs)**: The new DIM layer in IoTeX 2.0 offers a modular set of features that encompass the entire DePIN tech stack. While promoting contributions from global builders, the IoTeX coredev will provide in-house implementations for several layers. Additional DIMs like AI inference, storage, privacy-preserving compute, data analytics, RPC, and domain name systems will be provided by partners and builders who will stake IOTX to MSP. Note that each DIM can have its own token if necessary.

- **Public Goods**: IoTeX's goal is to bring DePIN to new frontiers, which requires public goods that anyone can trust and can freely utilize. Our goal is to lead the DePIN movement by creating a suite of open-source resources that builders can integrate with seamlessly and offer to their users to drive open participation. These public goods include user-facing tools (e.g., explorers, wallets, bridges), developer-focused tools (e.g., IDEs), and network-wide resources (e.g., governance, funding).

- **Meritocratic Tokenomics**: The addition of new layers to the IoTeX Network brings new stakeholders, which will contribute expertise across different categories. The goal of our refreshed tokenomics is not only to expand the utility of the IOTX token, but to do so in a meritocratic fashion where rewards are distributed based on the significance of a stakeholder's contributions. The expanded scope of the IoTeX Network will drive new utility to the IOTX token, making it the foundational currency of the DePIN sector.

- **DePIN Dapps & DePIN L2s**: At the top of the tech stack will be an ecosystem of DePIN Dapps and L2s that leverage some or all of the DIMs of IoTeX 2.0. While many Dapps will choose to launch their native tokens on the IoTeX L1 and utilize all of the DIM offerings, some Dapps may only choose to utilize one or more DIMs. The modular focus on IoTeX 2.0 enables Dapps to leverage different modules based on their current state needs, while making new capabilities available for their future needs. In addition, a new component of the DIM layer is the ioDDK, a L2 chain SDK which will enable projects to launch their own L2s on top of the IoTeX L1.

This will enable DePINs to create their own sovereign token economies and host their own Dapps, all while benefiting from the broad capabilities of the DIM layer and gaining security and trust from the IoTeX L1.

2.2 What We (Not) Build

As mentioned in Section 1.3, constructing a DePIN necessitates a multi-layered tech stack (see Figure 2.2), encompassing a broad range of capabilities. The newly introduced DIM layer of IoTeX 2.0 offers solutions for each of these tech stack elements. This DIM layer is entirely open, enabling any infrastructure builders to incorporate their implementations. This provides DePIN projects with a vast array of options for creating their custom tech stack.

Along with the core modules developed internally by the IoTeX coredev, numerous modules will be sourced from leading projects in the blockchain space with specialized capabilities. For instance, the Data Availability layer is the main focus of projects like Celestia and NEAR, whereas the Long-term Storage layer is the central focus of projects like Filecoin and Arweave. As IoTeX 2.0 stresses modularity and composability, we invite all projects to integrate into the DIM layer, thus enabling DePIN projects to design a tech stack of their preference.

While we openly welcome offerings into any part of the DIM layer, the IoTeX coredev has researched and developed state-of-the-art solutions for several critical modules focused on unified trusted layer for DIMs, hardware, identity, off-chain computing, L2 SDKs and public goods, which we summarize below and explore in detail throughout the following sections.

- **MSP (Unified Trusted Layer for DIMs)**: This is a unified trusted layer composed of a set of smart contracts on IoTeX L1. It takes staked IOTX and other mainstream assets and rents out its security to other DIMs.
- **W3bstream (Off-Chain Computing DIM)**: The world's first decentralized off-chain computing network that utilizes both in-house and third-party

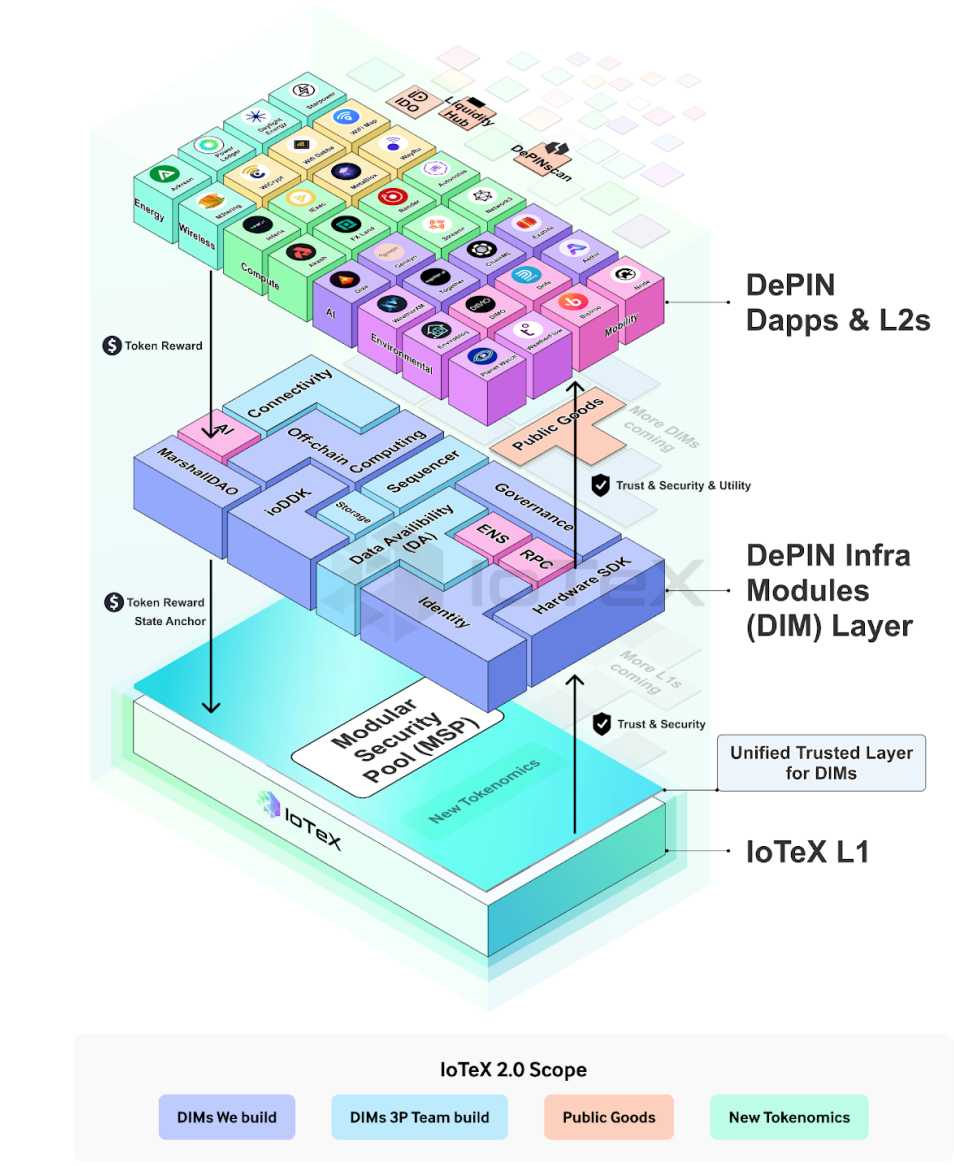

Figure 2.1: The Scope of IoTeX 2.0

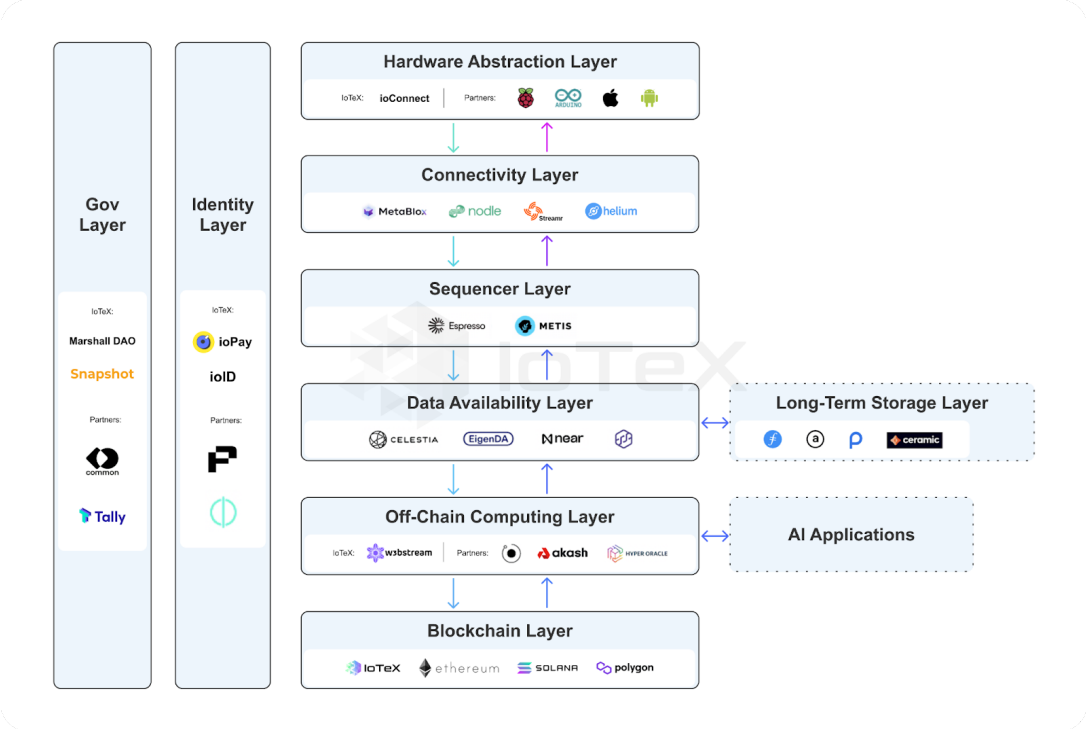

Figure 2.2: The DePIN Infrastructure Modules (DIMs)

verifiable computing technologies such as zero-knowledge proofs (ZKPs), trusted execution environments (TEEs), multi-party computation (MPC), and fully homomorphic encryption (FHE) for different vendors to generate "proofs of real world activity" in real-time, and settle these proofs to the blockchain to reward device owners.

- **ioID (Identity DIM)**: A suite of on-chain and off-chain self-sovereign digital identities that enable people and machines to establish rich digital relationships and interact with each other without relying on centralized identity providers.
- **ioConnect (Hardware Abstraction DIM)**: An SDK that enables various hardware to connect with W3bstream and various L1/L2s. It serves as

the hardware abstraction layer that works seamlessly on mainstream hardware platforms such as Raspberry Pi, ESP32, and Arduino, simplifying the complexity of dealing with hardware. In other words, devices powered by ioConnect can be easily integrated into various DePIN apps, serving as a multi-miner.

- **ioDDK (L2 SDK DIM)**: A chain SDK that enables DePIN builders to seamlessly start their own L2 blockchain while enjoying the security from IoTeX L1. It natively supports IoTeX modules such as W3bstream, ioID, and DePINscan.
- **IoTeX L1**: The IoTeX L1 blockchain is EVM-compatible and runs our in-house Roll-DPoS consensus mechanism to achieve 1,000+ TPS. The scope and utility of the IoTeX L1 will be expanded in IoTeX 2.0: ioIDs will be registered to the IoTeX L1, the MSP will be deployed as smart contracts on the IoTeX L1, and the ioDDK will anchor L2 chains to the IoTeX L1.
- **Public Goods**: We will continue to grow our existing public goods, such as DePINScan [23] and DePIN Liquidity Hub [21], as well as build public goods for DePIN builders.

2.3 Tokenomics

The IOTX token was introduced in 2019 as the underlying currency for the IoTeX L1. Since the launch of Mainnet, the IOTX token has effectively balanced incentives between validators (or "Delegates"), Dapp builders, and users. Delegates that stake IOTX and validate blockchain transactions as part of network consensus receive IOTX rewards, while developers and users comprising Dapps, token-holders, and more pay IOTX to send transactions and interact with smart contracts. IOTX tokens are also staked by various types of token-holders to participate in network-wide governance.

As IoTeX expands from simply an L1 to a modular platform of interconnected infrastructure, the tokenomics related to the IOTX token will also be expanded

to fit our vision for IoTeX 2.0. This includes new forms of utility for the IOTX token, which will be incorporated into the new technology offerings of IoTeX 2.0. In addition, another important goal of IoTeX 2.0 tokenomics is to balance inflationary staking rewards, deflationary burning of tokens based on platform usage, and incentivize DePIN Dapps and L2s to utilize our modular infrastructure. This means that our upgraded tokenomics will not only bring new utility and value to the IOTX token by linking it to W3bstream, ioID, ioDDK, and other DIMs, but also maintain a stable token supply through the balancing of inflationary and deflationary mechanisms. With increased adoption of IoTeX's modular infrastructure offerings, the IOTX token will accrue new value as the currency of the IoTeX 2.0 network.

2.3.1 IOTX Utility in IoTeX 2.0

IOTX tokens will be used across the entire IoTeX 2.0 infrastructure and ecosystem, and can be viewed from different perspectives, as illustrated in Figures 2.3 and 2.4.

- **From IoTeX L1 Perspective**: Delegates will stake IOTX to be eligible to validate network transactions and participate in consensus, and will receive IOTX tokens as rewards for their services. Token-holders may also stake IOTX to vote for Delegates and receive IOTX rewards. The IOTX token will continue to serve as the native currency of the IoTeX L1 blockchain in IoTeX 2.0, where Dapps that want to deploy smart contracts and process transactions on the IoTeX L1 blockchain will spend IOTX as gas fees. In addition to staking IOTX to participate in governance, users may also spend IOTX as gas fees to process transactions on the IoTeX L1 and interact with Dapps by contributing their capital and resources to earn rewards. In IoTeX 2.0, device owners may also burn IOTX to register their devices to the IoTeX L1 and receive ioIDs, which provide a trusted anchor for participation in DePINs. Finally, to create a flywheel, the IoTeX L1 will employ a DAO where token-holders may vote for how network incentives are allocated to

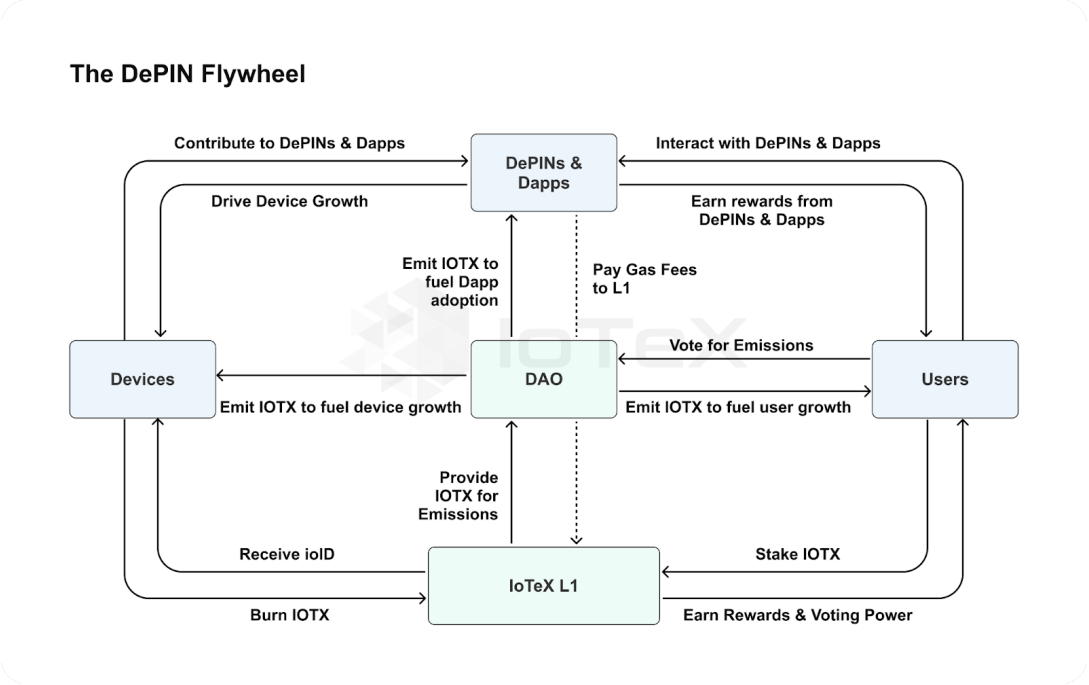

Figure 2.3: The DePIN Flywheel and Utility of IOTX Tokens

various initiatives with the goal of fueling new devices, DePINs, Dapps, and users. The more devices, DePINs, Dapps, and users are onboarded, the more utility IOTX will have on the IoTeX L1 via burning, staking, and spending of IOTX.

- **From Modular Security Pool (MSP) Perspective**: IoTeX 2.0 will enable users to repurpose their staked IOTX by re-staking or rehypothecating it to the Modular Security Pool (MSP), which is designed to extend the IoTeX L1 blockchain's security to DIMs that integrate their offerings to IoTeX 2.0. Using the MSP, DIM builders can incentivize IOTX stakers to allocate their re-staked IOTX to provide security to their solutions. This introduces a new economy incorporating staked IOTX where the MSP will effectively "lease" security and trust to DIMs, which will be required to stake IOTX. This also enables new earning opportunities for IOTX stakers, who will earn the same base IOTX staking rewards as well as additional rewards

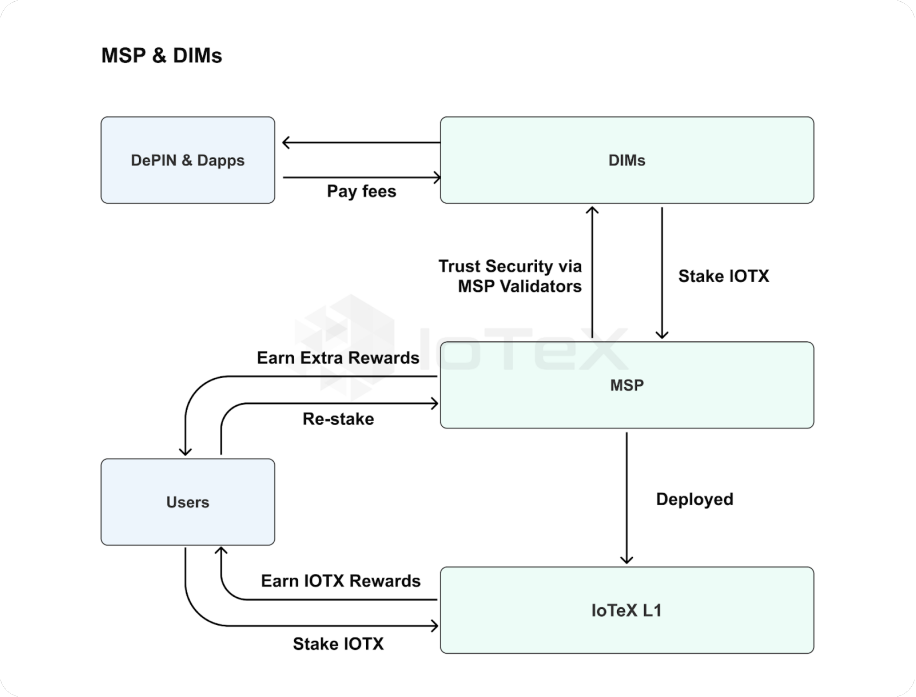

Figure 2.4: The Utility of IOTX Tokens in MSP and DIM

for re-staking their staked IOTX tokens, plus potential bribes from DIM projects.

- **From DePIN Infrastructure Modules (DIMs) Perspective**: DIMs will be required to stake IOTX in order to join the Modular Security Pool (MSP), gain security from the pool of re-staked assets, and offer their services in a verifiable fashion to Dapps, L2s, and users. DIMs may also choose to utilize IOTX as payment from Dapps that leverage their services, or they may utilize their own tokens. For example, a long-term storage provider like Filecoin or a data availability provider like NEAR would stake IOTX to join IoTeX 2.0 as a DIM, after which they could charge Dapps for their data services in their own tokens. For several of the IoTeX 2.0 DIMs that are built in-house by the IoTeX team, such as ioID and ioConnect, payment for these services will be denominated in the IOTX token.

- **From DePIN Dapps & DePIN L2s Perspective**: Dapps and L2s that launch on the IoTeX 2.0 tech stack will pay IOTX to process transactions and interact with smart contracts. In addition, Dapps and L2 chains may choose their own modular tech stack and pay one or more DIMs for services, such as connectivity, data storage, off-chain compute, and more, in the DIM's token. To close the loop, most Dapps will have their own tokens that users will acquire and spend to access the Dapps services.

In addition to the utility for IOTX token above, there are also new designs for IoTeX 2.0 regarding how IOTX tokens will be burned based on infrastructure usage, how IOTX will be shared with Dapps and builders via incentives programs, and how new IOTX will be emitted to stakers going forward, as shown in Figure 2.5. We explore these new designs in the following subsections.

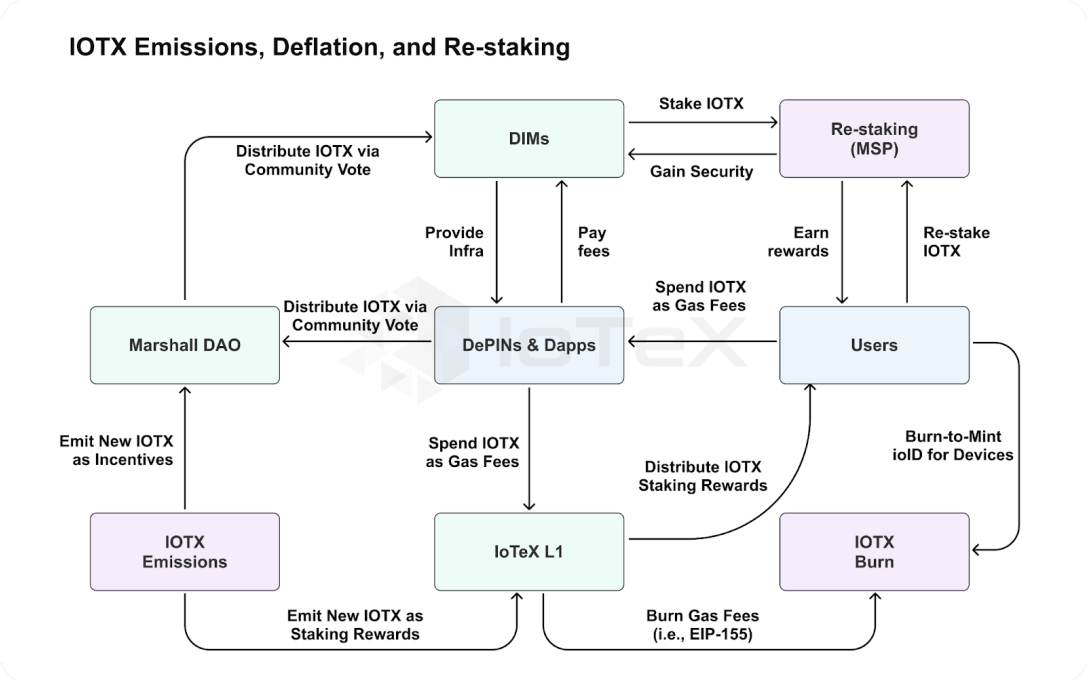

Figure 2.5: The Emission, Deflation and Restaking of IOTX Tokens in IoTeX 2.0

2.3.2 Inflationary Staking Rewards

When the IoTeX Mainnet was launched in 2019, 12% of the total IOTX supply (i.e., 1.2B IOTX) was allocated to staking rewards for Delegates. Token-holders stake IOTX in order to vote for Delegates that share a portion of the staking rewards with their voters. Since 2019, approximately 200M IOTX per year has been distributed to Delegates and voters in the form of block rewards and epoch rewards. Block rewards were delivered to Consensus Delegates (i.e., Top 36 voted Delegates eligible to produce blocks) for each new block produced, while epoch rewards were split proportionally across the Top 100 voted Delegates every epoch (i.e., every hour). After more than 4 years of Mainnet being live, the originally allocated IOTX supply for staking rewards is nearing full distribution. As such, inflationary staking rewards will be introduced as part of IoTeX 2.0 to incentivize Delegates to continue validating network transactions and securing the network.

Inflationary staking rewards are defined as new IOTX added to the token supply, delivered to Delegates that participate in consensus and token-holders that stake IOTX. Essentially, this means only those that stake IOTX tokens will receive the newly minted IOTX tokens, which drives a higher staking ratio of IOTX and higher security for the IoTeX network overall. The distribution of inflationary staking rewards will follow the same structure as the previous distribution of IOTX allocated to staking rewards, where Consensus Delegates that produce blocks will earn block rewards and the Top 100 Delegates will proportionally split epoch rewards.

While this is a new concept for the IoTeX Network, inflationary staking rewards are built-in to almost all L1s, including Ethereum, Solana, Cosmos, and more. For example, Solana began with an 8% inflation rate, which reduces 15% each year; as of Q1 2024, the Solana Network has $\sim$5.5% inflation. While the actual percentage of annual inflation for the IoTeX Network will be determined by network-wide governance, the goal will be to introduce mild inflation that provides competitive staking rewards APRs for IoTeX L1 delegates compared to other blockchain ecosystems, and incentivize DIMs and DePIN apps to grow while maintaining

a stable token supply when taking deflationary burning of tokens into account, which is detailed in the section below.

2.3.3 Deflationary Burning

To balance necessary inflation in crypto networks, deflationary burning of tokens based on network usage is commonly implemented to maintain a stable token supply (e.g., Burn and Mint Equilibrium is such a design pattern). For example, the Ethereum Network issues approximately 1,700 new ETH per day to validators but balances this inflation with deflationary burning of gas fees (i.e., EIP-1559) to maintain an overall stable or deflationary ETH token supply over time. Since 2020, the IoTeX Network utilized the Burn-Drop program to drive deflationary burning of IOTX based on the number of new devices registered to the network, resulting in approximately 4% of the total supply or 400M IOTX being burned to date. With the introduction of IoTeX 2.0 and the sunsetting of the Burn-Drop program, new sources of deflationary burn will be added to the IoTeX Network at the protocol level based on the usage of our modular infrastructure.

- At the L1 level, IoTeX 2.0 will introduce the burning of gas fees similar to Ethereum's EIP-1559. This will incentivize and redistribute value to IOTX token-holders based on the increased usage of the IoTeX L1. The staking of IOTX to participate in governance and vote for Delegates will remain unchanged, maintaining the important effect of staked assets reducing the velocity of the IOTX token.
- For ioID, the creation of new on-chain identities for devices will require a certain amount of IOTX to be burned, where the rate of burn will be dynamic based on the total number of devices registered to the IoTeX Network. In addition, the design of ioID will incorporate an additional deflationary burn mechanism to obtain Verifiable Credentials (VCs) for DIDs. As an analogy, an ioID is similar to an empty passport while VCs are similar to stamps for a passport that enable people to access various countries.

In IoTeX 2.0, ioIDs will be registered to the IoTeX L1 and one or more VCs for devices will be obtained by burning IOTX tokens to access DIMs like W3bstream. This design will redistribute value to IOTX token-holders based on the growth in the number of "equipped" devices in the IoTeX Network, similar to Burn-Drop but redesigned to better align with IoTeX 2.0's modular design.

- For W3bstream, ioConnect, and ioDDK, the network effects fueled by the growth and adoption of these modular products by Dapps and companies will drive deflationary burning of IOTX due to the need for devices to interact directly with each respective DIM. In addition, periodic burning of IOTX tokens based on adoption thresholds defined by the IoTeX community may be instituted to re-distribute value to token-holders.

IoTeX 2.0 tokenomics are designed to reward the increased usage of the various modular components of the IoTeX platform by driving the deflationary burning of IOTX tokens. Initially, this deflationary burn will counterbalance the inflationary staking rewards mentioned above to maintain a net stable total token supply, and in the future mass adoption of the IoTeX platform could drive the total IOTX token supply to be net deflationary. To fuel the mass adoption needed to achieve this, IoTeX 2.0 tokenomics will allocate IOTX tokens to a variety of builders via growth incentive programs described below.

2.3.4 Growth Incentives

An important pillar of IoTeX 2.0 is the Marshall DAO (IIP-23) [10], a Decentralized Autonomous Organization (DAO) that will enable IoTeX stakeholders to make proposals regarding how to allocate IOTX incentives to grow the IoTeX ecosystem, including onboarding reputable DePIN projects and funding network-wide initiatives. This creates a transparent and meritocratic system where the best ideas are funded using IOTX. The Marshall DAO will initially be funded by more than 500M IOTX that was repurposed from the Burn-Drop allocation,

which was decided by the IoTeX community via a network-wide vote in Q1 2024. In the future, additional funding for the Marshall DAO may be added via further network-wide votes to add newly minted IOTX to the pool.

As shown in Figure 2.6, the Marshall DAO employs a vote-escrow on-chain governance model, which means the more IOTX is staked in the DAO the more voting power a user has. This ensures decisions to fund projects and initiatives are made by those who are most invested in the long-term success of IoTeX. Token-holders that stake for at least 91 days will earn veIOTX, a non-transferrable on-chain token, which can be used to propose and vote on funding allocations via gauges that represent specific proposals. This means long-term stakers can vote using their veIOTX to shape how IOTX from the DAO funds various projects, including but not limited to boosting liquidity for DEX trading pairs on IoTeX, sponsoring early-stage DePIN projects via launchpads, accelerating DePIN projects via dual-mining, issuing grants for public goods and network-wide tools, and more.

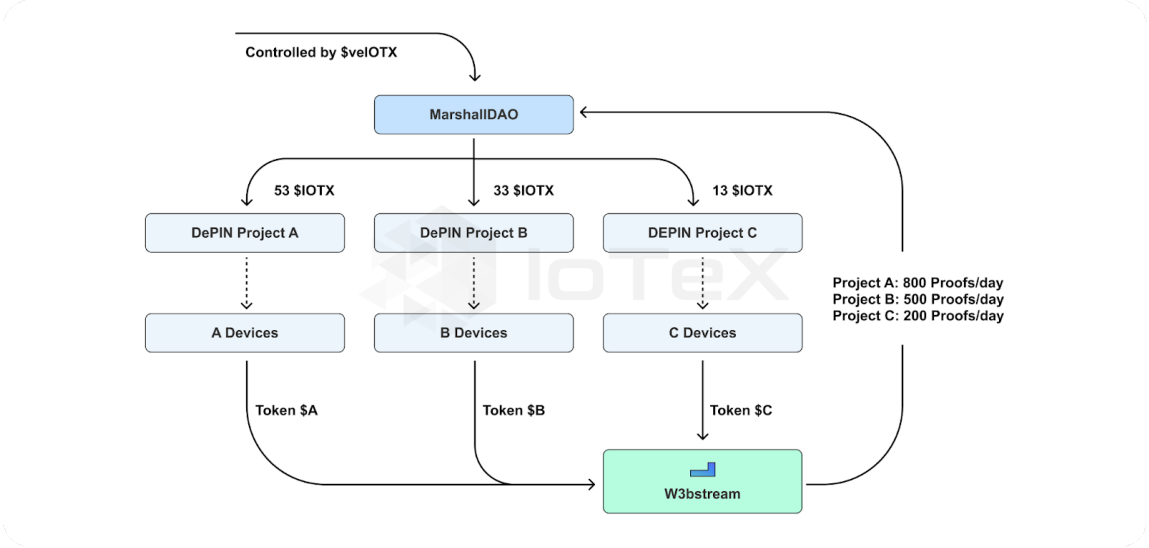

Figure 2.6: The Marshall DAO Governance Model

2.4 Public Goods

In addition to capabilities provided by the IoTeX blockchain and DIMs, public goods that address many of the near-term and medium-term challenges of DePIN projects are also an important part of IoTeX 2.0. These public goods provide awareness, usability, and liquidity to DePIN projects through simple integration, as well as provide the IoTeX community a way to monitor the broader DePIN industry as well as deep-dive on specific projects.

- DePINScan [23] is an industry-wide explorer for the DePIN sector (see Figure 2.7). It is designed to empower users, miners and investors in DePIN to monitor the growth of DePIN projects and discover early-stage projects. It provides real-time device counts and project profiles, serving as a way to discover projects and obtain real-time price, volume, and market cap for DePIN assets.

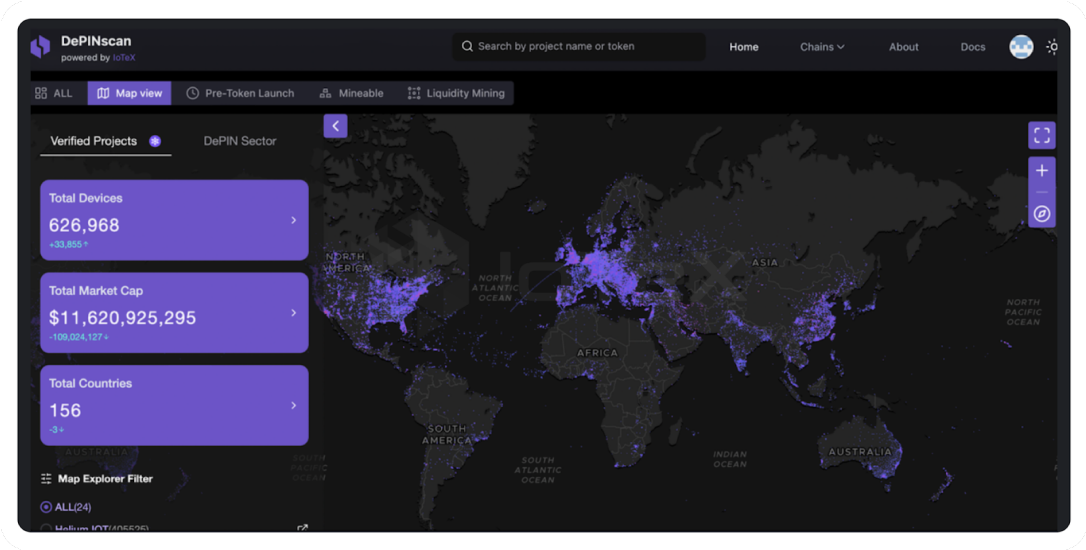

Figure 2.7: The DePINScan Explorer

- DePIN Liquidity Hub [21] is a Uniswap v3-type DEX with concentrated liquidity that provides for automated range managers (market makers) and

allows users to trade DePIN tokens (see Figure 2.8). Token liquidity is highly important to any crypto project, especially DePINs, as they utilize their token heavily as an incentive mechanism to grow their network. Unfortunately, many early-stage DePINs struggle to create and maintain healthy levels of on-chain liquidity. To support new projects, IoTeX has launched the DePIN Liquidity Hub [24] to increase liquidity for DePIN projects who can bridge their tokens from any other L1 chain to the IoTeX L1, create a two-sided liquidity pool on various decentralized exchanges (DEX), and run liquidity mining campaigns to incentivize investors to bootstrap their on-chain liquidity.

Figure 2.8: The DePIN Liquidity Hub

In addition to the public goods above that are already available to builders, there are others that will be built by the IoTeX team as well as global builders throughout the development of IoTeX 2.0. The examples are launchpad for DePIN projects to bring their projects to passionate investors, device marketplaces to expose DePIN-focused hardware to miners, and governance tools to enable

decentralized voting for DePIN projects. With the public goods readily available for builders, IoTeX 2.0 will empower projects with a full suite of capabilities to make launching and growing a DePIN project easier than ever.

2.5 Support Builders Throughout Project Life Cycle

IoTeX 2.0 offers a full range of infrastructure, tools, and public resources, all governed by meritocratic tokenomics. These are designed to assist DePIN builders at every phase of their project lifecycle, as shown in Figure 2.9.

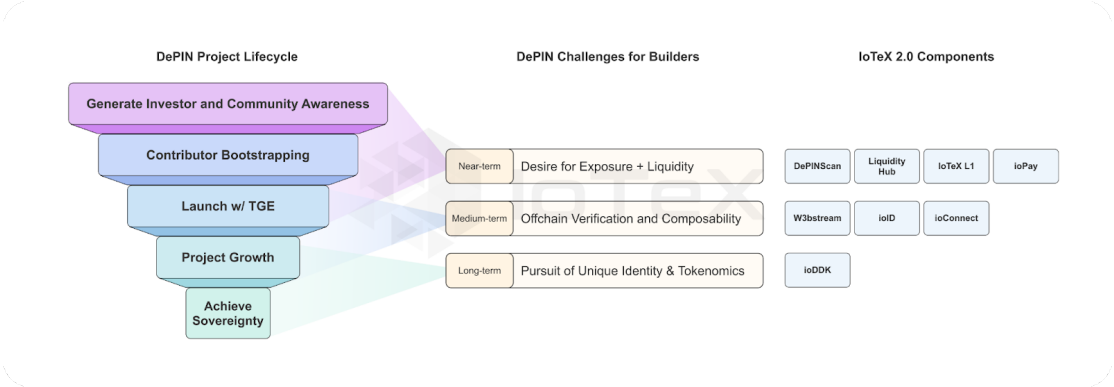

Figure 2.9: Support Builders throughout DePIN Project Lifecycle

- In the initial stages, DePIN projects mainly focus on developing their tech stack and creating awareness for their projects. To facilitate this, IoTeX 2.0 provides public resources like DePINscan and Liquidity Hub to capture attention, liquidity, and users.
- As projects progress, the demand for more advanced and adaptable infrastructure increases, especially as projects decentralize their tech stacks and aim for more scalability. To cater to these needs, IoTeX 2.0 offers infrastructure such as W3bstream, ioID, and ioConnect to provide cutting-edge technology for DePIN builders.

- In the long-term, DePIN projects need to establish and expand their own sovereign networks of supply and demand. IoTeX 2.0 continues to support these projects even in their later stages by allowing them to launch their own L2 via ioDDK.

2.6 The Future

With IoTeX 2.0, we are embarking on a new journey to equip the world's devices with all of the tools they need to be self-sovereign, compile real world intelligence to power innovative Dapps, and allow users to monetize the unique services and intelligence from their devices. The ongoing convergence of artificial intelligence, blockchain, and smart devices is now sparking a technological revolution that will fundamentally transform the way our world works. Although these technologies have evolved independently over time, they are becoming increasingly intertwined and packaged into a new productive asset: DePIN networks composed of trusted and user-owned devices.

Smart devices will provide services and generate data. Blockchain will add trust and verifiability to these data and services. And finally, AI will extract value from the data and automate these services. What seemed like science fiction only a few years ago is now becoming a reality. In the near future, the emerging machine economy will be driven by this technology trinity and become the most valuable industry in the world. With blockchain, we will have the ability to program this new machine economy with trusted technology that not only benefits society but also provides value and equity to everyday people. The possibilities are endless, but some of the most exciting opportunities are:

- **Collective Intelligence & AI**: IoTeX will become the largest device hub, and thus real world data hub, for aggregating real-time information. By capturing data streams from devices and verifying real world events on-chain, we can crowdsource the collective intelligence of the masses to revolutionize individual industries like connectivity, smart city, and renewable energy. An

even greater opportunity lies in utilizing AI to analyze cross-industry relationships and extract relational insights that can evolve our understanding of the world. IoTeX 2.0 will become the decentralized platform that records the history of the real world through the eyes of our smart devices, enabling us to understand our past so we can optimize our future.

- **Autonomous Machine Economy**: In addition to generating valuable data, smart devices are now evolving to deliver trusted and valuable services to people. Autonomous taxis are delivering the first driverless rides, satellites are providing connectivity to people across the world, warehouses are utilizing robots that exceed the dexterity of people, and solar and wind energy is being produced by next-gen renewable energy devices. The orchestration of these service-delivering devices is best performed with blockchains and intelligent AI. We envision a future where IoTeX can enable AI systems to monitor and manage the Earth's resources with unprecedented precision and full trust.

- **Digital Resource Marketplaces**: While some DePINs focus data and services from location-dependent hardware, others aggregate digital resources from location-agnostic hardware. These may include digital storage, compute via CPUs and GPUs, bandwidth, and other digital resources traditionally offered by Cloud conglomerates. In an era where "data is the new gold" and "compute is the new oil", IoTeX 2.0 will enable the crowdsourcing of valuable digital resources into marketplaces where anyone can exchange them in a peer-to-peer fashion with others around the world.

- **Decentralized Governance & Decision-making**: By integrating real-world data into blockchains securely and transparently, IoTeX 2.0 can help establish the foundation for decentralized decision-making using verifiable facts about events in the real world. With humans collectively defining processes via decentralized governance, we can utilize immutable smart contracts and secure devices to operate major aspects of society in a trusted fashion. IoTeX 2.0 provides an avenue for anyone to contribute their expertise and

participate in open governance of the new world.

Chapter 3

Modular Security Pool (MSP) - A Unified Trusted Layer for DePIN Infrastructure Modules

3.1 The Problem

DePIN features a comprehensive tech stack that includes both on-chain elements like scenario-specific DePIN L2s and off-chain elements such as data streams, oracles, processes, verification, storage, and automation. This complex structure necessitates more modules and builders to create their own decentralized trust architectures from scratch. Tasks may include designing a staking token, creating liquidity, attracting stakers, recruiting validators, and gaining market adoption, leading to potential fragmentation of security and decentralization.

For establishing a unified and end-to-end trust in a decentralized manner, it's crucial to ensure that each part is as secure and decentralized as possible, following the weakest link principle. As builders continue to develop DePIN Infrastructure Modules (DIMs), maintaining the integrity of security and decentralization without fragmentation is a priority. This approach allows for swift integration of DIMs into the existing tech stack for use in DePIN projects.

The Modular Security Pool (MSP) provides a unified trust layer that supports the DIMs. It collects staking security from various established L1/L2s and may lend their security to new DIMs in exchange for compensation. This system enables new infrastructure modules to benefit from the security of underlying L1/L2s without building their own security infrastructure. For instance, a new DIM can join the MSP through a governance proposal. If approved, the DIM will adopt the security and decentralization of the L1/L2s and receive usage of their protocols from IoTeX ecosystem projects. Stakers who support a particular DIM by directing their stakes to the MSP may receive compensation in the form of DIM network tokens.

3.2 Open Market for Security and Trust

The MSP confidently presents an open market mechanism, masterfully governing the supply and consumption of its pooled security by stakers and DIMs. MSP will consolidate DePIN-focused security across all DIMs, instead of fragmenting security among numerous DIMs. Concretely, there are three types of participants in MSP:

- **DIM Builders** build DIMs such as scenario-specific DePIN L2s, off-chain services like data streaming, oracle, processing (like general-purpose, ZKP-based, TEE-based, etc.), data storage, automation (such as auto payout, price feeds),identity, and authentication modules. DIM builders must incentivize stakers to allocate their assets to their modules. MSP will provide a bribe mechanism to make sure the stakers are sufficiently incentivized from DIMs.
- **Stakers** are network participants who delegate their assets from well established blockchains to one or more validators. They contribute to network security without having to run a node themselves. In return for their delegation, they earn a portion of the network's fees and rewards. Strategic

allocation determines modules deserving of extra pooled security, considering potential for more slashing. Stakers opt in by allowing MSP to impose extra slashing conditions on their assets, enhancing economic security. It's important to note here that the MSP infrastructure we are building is open-source and will be able to leverage security from the IoTeX L1 in the near term and all major blockchains, including Bitcoin, Ethereum, and Solana in the future.

- **Validators** provide an always-running set of nodes available to DIM builders that would directly serve DePIN projects.

The implementation of MSP should incorporate the following key principles:

- **Open entry and exit**: Stakers and DIMs should have the freedom to enter and leave the market without any restrictions. This ensures competitive pricing, reflecting the true value of services.
- **Network effects**: As the number of participants increases, each participant finds the market more valuable. This positive feedback loop can draw more buyers and sellers to the market.
- **Permissionless**: The market is not controlled by a central authority. Instead, it operates based on the laws of supply and demand.

3.3 Architecture

As shown in Figure 3.1, the architecture of the Modular Security Pool (MSP) is designed to provide a streamlined and secure process for building new networks, specifically DePINs and DIMs, based on inherited security from existing staking systems on well established L1 blockchains. Here's a detailed breakdown of how the MSP operates:

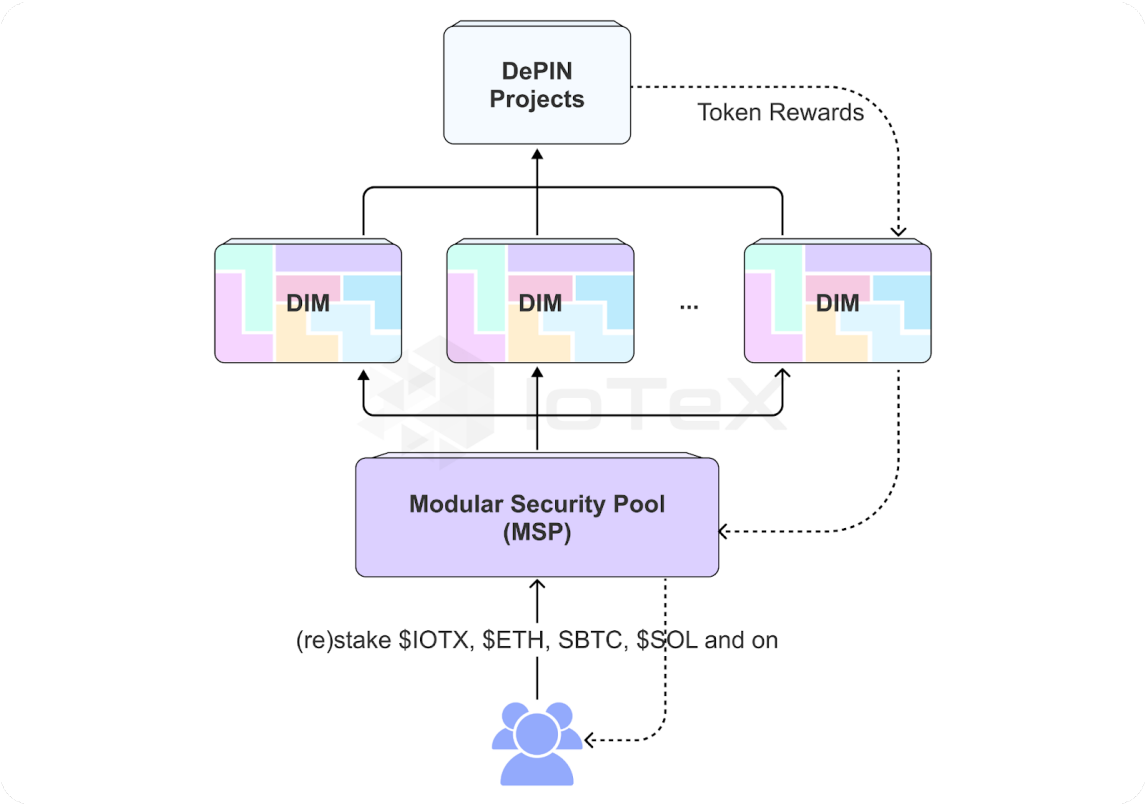

Figure 3.1: The Architecture of the Modular Security Pool (MSP)

1. **Stakers Delegate Assets**: Stakers, who are participants in established L1s such as Bitcoin, Ethereum, and IoTeX, delegate their assets to the MSP. By doing so, they contribute to the security of MSP-powered networks.

2. **Stakers Choose Validators**: Within the MSP network, stakers have the flexibility to choose validators from a pool of options provided by DIM networks they are associated with. Validators are responsible for running nodes to secure the network and validate transactions.

3. **Validators Run Nodes**: Once selected by stakers, validators operate nodes within the MSP network. These nodes play a crucial role in ensuring the integrity and security of transactions across the network.

4. **DIM Builders Establish Networks**: Meanwhile, DIM builders work on developing their respective networks.

5. **Incentivizing Stakers**: DIM builders incentivize stakers to allocate their assets to their modules within the MSP network. This incentivization can take various forms, such as rewards, network tokens, or other benefits. The MSP ensures that stakers are sufficiently motivated through mechanisms such as a bribe mechanism to encourage participation.

6. **Distribution of Staking Security**: The MSP plays a pivotal role in distributing staking security to new DIMs. By leveraging the pooled security gathered from established L1/L2s and the participation of stakers and validators, the MSP serves the security and decentralization of these new networks.

Overall, this architecture facilitates a more efficient and secure process for launching new DIMs. By leveraging the security of existing L1/L2s and integrating various stakeholders such as stakers, validators, and builders, the MSP fosters a robust ecosystem conducive to innovation and growth in decentralized trust architectures. This approach not only saves time and resources for new network developers but also strengthens the overall security and resilience of the DePIN ecosystem.

Chapter 4

W3bstream - A Decentralized Multi-Prover Network for DePIN Verification

DePIN applications usually contain a dedicated data processing scenario (e.g., compute a score, locate a device, detect fraudulent devices, etc.) that is able to extract insights based on data collected by DePIN devices from the real world. The insights are then used to trigger smart contracts for token-related actions. Due to the high volume of machine data, processing and storing it on-chain is prohibitive and inefficient. As a result, off-chain computing has emerged as a promising solution to addressing the scalability challenges in DePINs.

4.1 W3bstream Architecture

W3bstream is a blockchain-orchestrated multi-prover network developed by IoTeX, which aims to harness the power of global-scale heterogeneous provers to supercharge emerging DePIN applications. In a nutshell, W3bstream is a decentralized off-chain computing network that is composed of heterogeneous nodes

performing verifiable computations, as illustrated in Figure 4.1. The proofs generated by W3bstream are verified with the on-chain verifiers and then consumed by DePIN dApps.

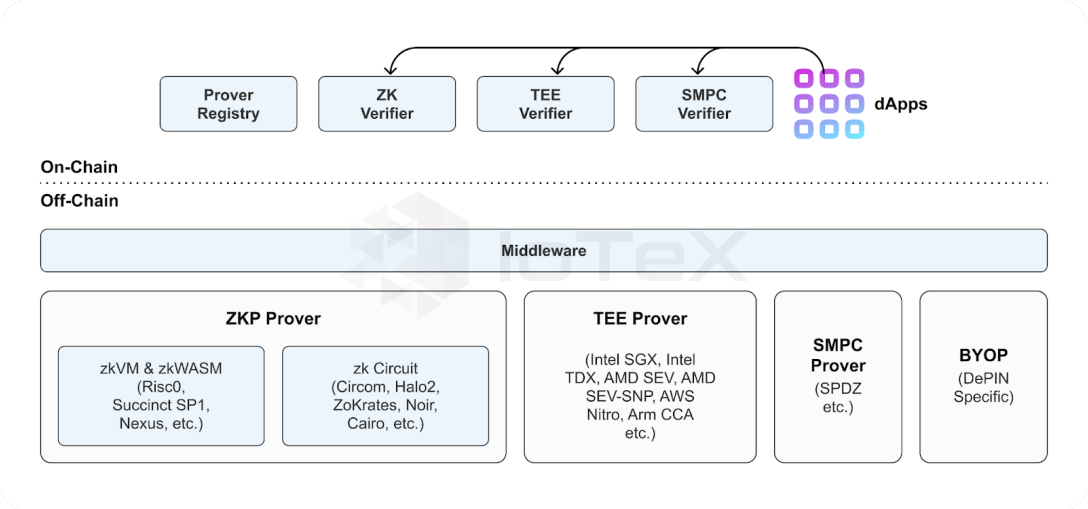

Figure 4.1: W3bstream in a Nutshell

4.1.1 Four Types of Provers

A number of techniques have been developed in the past to attest integrity of data processing and allow public verifiability, including zero-knowledge proofs (ZKPs), trusted execution environments (TEEs), secure multi-party computations (SMPCs). These technologies rely on various security assumptions and have different implications in practice. W3bstream is able to accommodate four categories of provers to realize verifiable computation for DePIN applications, namely zero-knowledge proof (ZKP) Prover, trusted execution environment (TEE) Prover, secure multi-party computation (SMPC) Prover and Bring Your Own Prover (BYOP), via the well-designed middleware layer.

- **ZKP Prover**: A ZKP allows one party (i.e., a prover) to prove to another party (i.e., a verifier) that a given statement is true, without disclosing

additional information beyond the fact that the statement is true. ZKPs need to satisfy the formal requirements of completeness, soundness, and zero-knowledge, thereby enabling one to build trustless applications. In practice, a ZKP prover can be realized using either a general-purpose zero-knowledge virtual machine (zkVM) or a customized constraint system (i.e., a circuit). A typical system architecture of a SNARK-based application which is built upon a zkVM (resp. a customized circuit) is illustrated in Figures 4.2 and 4.3.

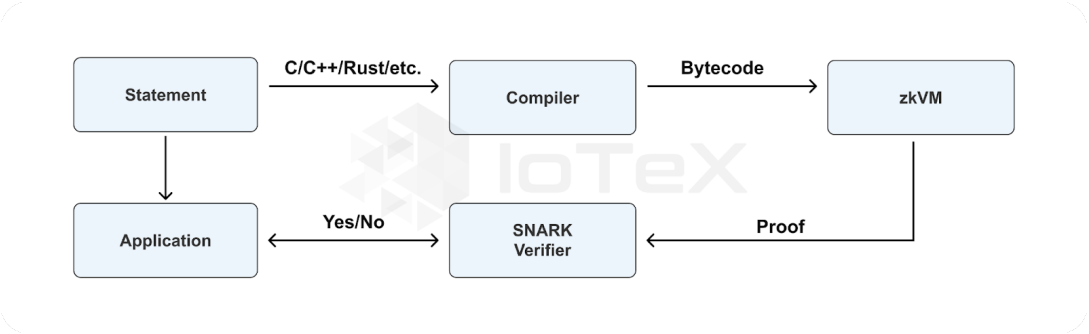

Figure 4.2: The System Architecture of a SNARK-Based Application Built upon a zkVM

While a general-purpose zkVM-based prover encapsulates the complexity of generating ZKPs and allows developers to code their business logic using high-level programming languages such as C/C++, Rust, etc., building a ZKP prover with a customized circuit requires a deeper understanding of the ZKP generation workflow as well as domain-specific languages (DSLs). However, a ZKP prover with a customized circuit usually can achieve better performance when compared to that of a zkVM-based prover. The ZKP prover enables DePIN developers to leverage powerful ZKP technology for conducting trustless off-chain computing. W3bstream will gradually support the leading zkVM/zkWASM projects (e.g., Risc0 [28], Succinct SP1 [29], Nexus [30], zkWASM [31], etc.) as well as popular DSLs (e.g., Circom [32], Halo2 [33], ZoKrates [34], Noir [35], Cairo [36], etc.) for building customized zk circuits.

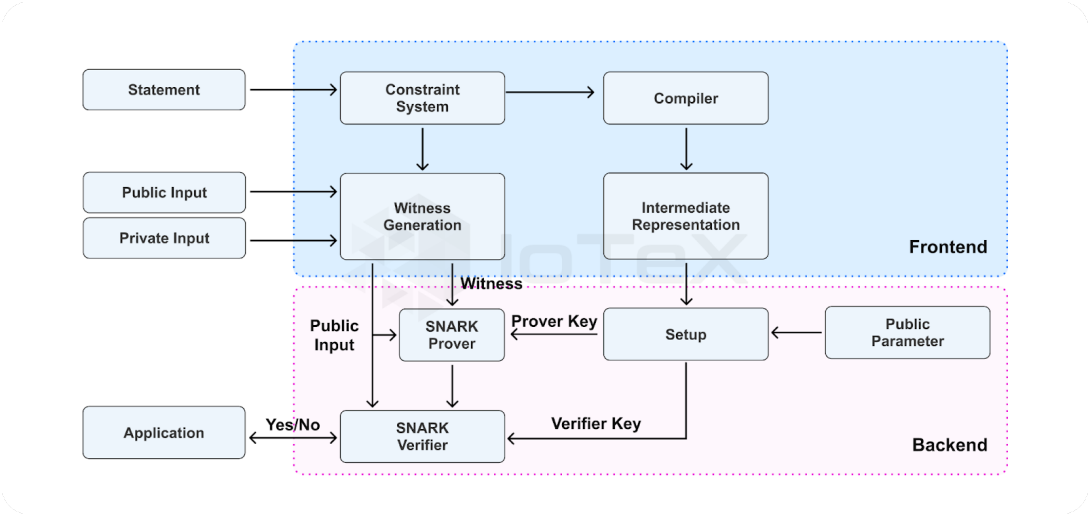

Figure 4.3: The System Architecture of a SNARK-Based Application Built upon a Customized Circuit

- **TEE Prover**: According to the definition by Confidential Computing Consortium (CCC), a trusted execution environment (TEE) is a dedicated hardware (and software) environment that provides a level of assurance of the following three properties: 1) Data Confidentiality: Unauthorized entities cannot view data while it is in use within the TEE; 2) Data Integrity: Unauthorized entities cannot add, remove, or alter data while it is in use within the TEE; and 3) Code Integrity: Unauthorized entities cannot add, remove, or alter code executing in the TEE. These salient security properties ensure the confidentiality and integrity of both data and program, thereby allowing a remote party to trust the computation results on a TEE-enabled hardware platform (e.g., Intel SGX, AMD-SEV, Arm CCA, AWS Nitro, NVIDIA H100, etc.). TEE-based systems root their security in hardware and users have to trust that the hardware has not been tempered with or is broken in an undetectable manner.

  A typical system architecture of a TEE-based application is shown in Figure 4.4, which relies on the remote attestation mechanism of a TEE-based hardware platform. Remote attestation is a process by which one party

(i.e., a verifier) assesses the trustworthiness of a potentially untrusted remote peer (i.e., an attester). The goal of attestation is to allow the verifier to gain confidence in the trustworthiness of the attester by obtaining an authentic, accurate, and timely report about the software and data state of the attester. With the aid of an attestation service, an attestation report can be obtained which contains the cryptographic measurement of the execution environment (i.e., hardware, software, custom data, etc.).

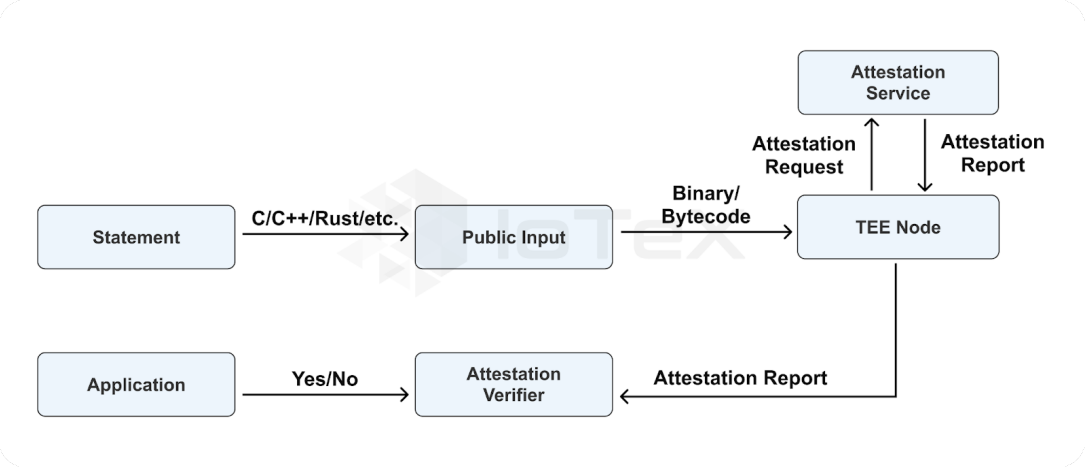

Figure 4.4: The System Architecture of a TEE-Based Application

A TEE prover can be implemented by following the general development flow of a certain TEE provider. The TEE prover facilitates DePIN developers to utilize the state-of-the-art confidential computing technology for performing privacy-preserving off-chain computing. W3bstream will gradually support the development flow of the leading TEE-based hardware platforms such as Intel SGX [37], Intel TDX [38], AMD SEV [39], AMD SEV-SNP [40], AWS Nitro [41], Arm CCA [42], etc.

- **SMPC Prover**: MPC represents a collection of techniques for privacy-preserving collaborative computations over distributed data and reveals nothing but the computation result. Given various security assumptions and threat models (e.g., semi-honest adversaries, malicious adversaries, covert ad-

versaries), a SMPC protocol should at least satisfy three properties, namely input privacy, correctness and independence of inputs. A typical system architecture of a SMPC-based application which is built upon a pre-processing model is shown in Figure 4.5.

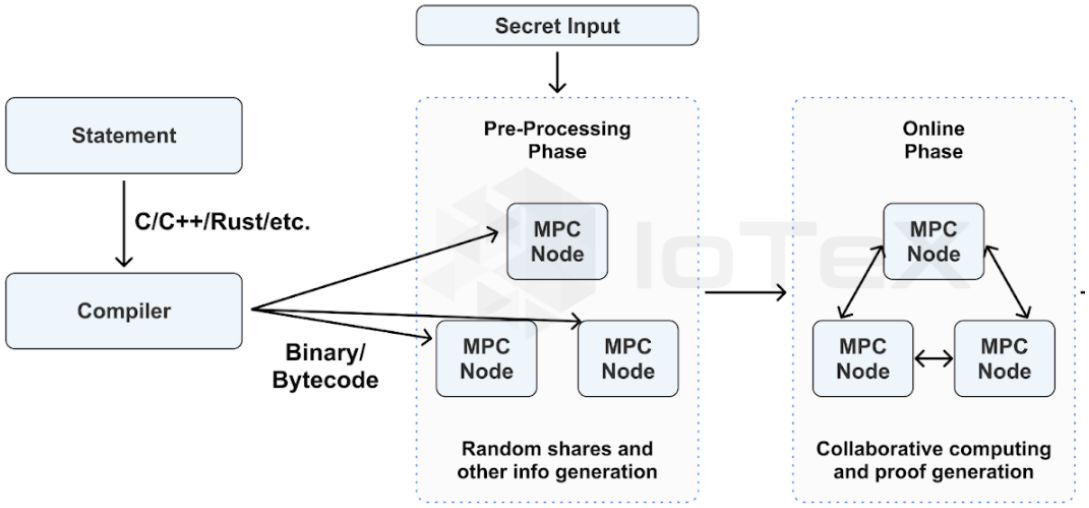

Figure 4.5: The System Architecture of a SMPC-Based Application

A SMPC prover can be realized by following the general development flow of a specific SMPC protocol (e.g., SPDZ). However, achieving public verifiability in an efficient manner is still an ongoing research direction.

- **Bring Your Own Prover (BYOP)**: The BYOP offers great flexibility for DePIN developers deploying optimized provers that are tailored to specific DePIN projects or exploring new efficient verifiable computation techniques in the context of DePIN.

4.1.2 Our In-house Innovation on ZKP

Multi-scalar multiplication (MSM) is one of the core components of many zero-knowledge proof systems, and a primary performance bottleneck for proof gen-

eration in these schemes. One major strategy to accelerate MSM is utilizing precomputation. Several algorithms (e.g., Pippenger [11, 12] and BGMW [13]) and their variants have been proposed in this direction. In our recent research [15], we revisit the recent precomputation-based MSM calculation method proposed by Luo, Fu and Gong at CHES 2023 [14] and generalize their approach. In particular, we presented a general construction of optimal buckets. This improvement leads to around 15% $\sim$ 40% performance improvements, which are verified by both theoretical analysis and experiments. We also introduced a bucket-amenable recording using fast endomorphisms on $j = 0$ elliptic curves to divide the storage requirement by 3, at almost no performance penalty, compared to our LFG already optimized algorithm.

4.2 W3bstream Workflow

4.2.1 Prover Onboarding and Management

The prover onboarding is based on ioID and follows the process described in Section 5.2.2 - ioID Registration and Binding. An on-chain fleet management contract is responsible for scheduling tasks and tracking the lifecycle of all the prover nodes. Each prover node can be either in a 'Busy', 'Idle' or 'Offline' status and the node status will be continuously updated in the fleet management contract. A W3bstream explorer can be used to check the status of all prover nodes.

4.2.2 Workflow

In a modular DePIN infrastructure, W3bstream is an implementation of the off-chain computing layer (OCCL) featuring multiple provers as described in Section 4.1. W3bstream is a decentralized heterogeneous prover pool that is able to perform a project-specific business logic on the data stored in the data availability

layer (DAL) and generating validity proofs (e.g., zero-knowledge proofs, attestation reports, etc.) of the computations executed. W3bstream works as a stateless computing component in a modular DePIN infrastructure and follows the high-level OCCL workflow as illustrated in Figure 4.6 below.

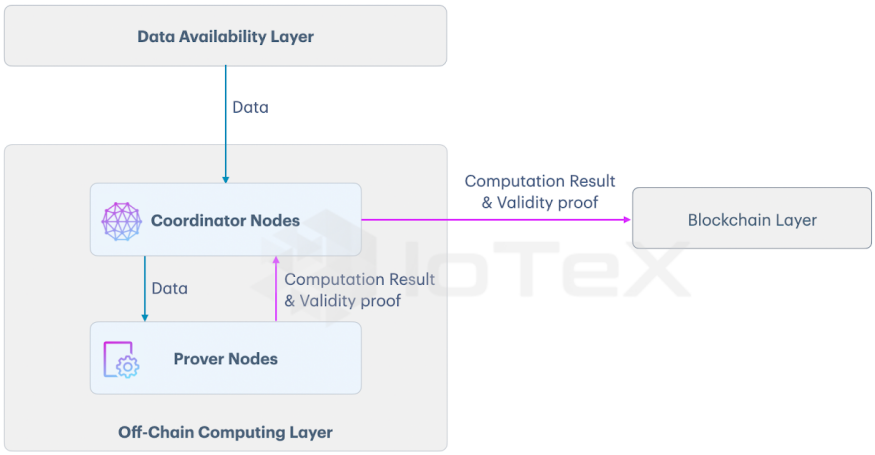

Figure 4.6: The High-Level Workflow of the Off-Chain Computing Layer

1. A coordinator node in the off-chain computing layer retrieves data from the data availability layer based on the configuration of a DePIN project;
2. The coordinator node feeds data to an idle prover node or a selected set of idle nodes in the off-chain computing layer;
3. The prover node(s) performs computation specified by the DePIN project and generates the computation result and corresponding validity proof;
4. The computation result and validity proof are returned to the coordinator node;

5. The coordinator node sends the computation result and validity proof to a smart contract for further processing.

Once a proof is verified on-chain successfully, the computation result can be trusted and consumed by the dApp of a DePIN project.

4.3 DePIN Verification and Off-Chain AI

The comprehensive suite of provers available in W3bstream allows a developer to prove integrity of off-chain computations to layer-1 blockchain for a wide range of DePIN applications. In particular, a developer can choose the most suitable verifiable computation technique for a specific application.

4.3.1 DePIN Verification

As Guy Woullet of a16z has pointed out [43], the success of DePIN hinges on addressing a pivotal challenge: ensuring trusted verification of geographically dispersed service nodes without the need for central authority. The current technology for DePIN verification can be roughly classified into three categories [44], namely trusted hardware based approach, statistical approach, and validity proof based approach. Each verification approach has its own pros and cons and a combination of multiple approaches might be required in practice. W3bstream facilitates various DePIN projects to deploy and subsequently update their verification algorithm on the platform. These verification algorithms can be written in high-level programming languages such as Rust, Golang, C++, etc. By using one of the provers provided in W3bstream, the trustworthiness of DePIN verification algorithms can be guaranteed.

4.3.2 Off-Chain AI

DePIN applications unlock new opportunities for AI training and inference across different industry sectors. On the one hand, DePIN applications are able to bring

huge amounts of real-world data to Web3 in a trustworthy manner, which could improve AI models' accuracy significantly. On the other hand, DePIN applications can effectively organize computing and storage resources for AI training and inference on a global scale. However, AI applications are often computationally intensive and pose significant challenges to be deployed on-chain. W3bstream allows a developer to conduct off-chain AI computations and ensures trustworthiness of the computation process simultaneously. While zero-knowledge proofs are able to provide strong integration protection for off-chain computing, applying zero-knowledge proofs for AI (e.g., ZKML) might easily incur 10,000x to 100,000x overhead when compared to non-verifiable AI computations [45]. In lieu of using a ZKP prover, a developer could switch to a more efficient TEE prover for off-chain AI computations in W3bstream. Our initial work [7, 8] built upon Arm's Veracruz framework and AWS's Nitro enclave has shown some very promising results.

Chapter 5

ioID - A Unified Identity System for DePIN

DePIN applications involve extensive on-chain (i.e., staking, asset transfer, lending, etc.) and off-chain (i.e., person-to-machine and machine-to-machine) interactions among different system participants. The identity layer in a modular DePIN infrastructure is an essential component to manage relationships of various entities and ensure secure interactions among them. As a result, designing a unified identity layer that is able to meet the requirements of both on-chain and off-chain interactions is highly desirable for DePIN applications.

5.1 On-Chain vs. Off-Chain Identity

5.1.1 On-Chain Identity

The primary goal of an on-chain identity is to attest ownership of crypto assets and perform a variety of crypto asset related operations such as transfer, staking, lending, etc. A blockchain address of an Externally Owned Account (EOA) or a Smart Contract Wallet (SCW) as specified in ERC-4337 [25] serves well for this purpose. In particular, a SCW that allows arbitrary verification logic is able to

abstract the complexities of blockchain transactions (e.g., signature verification, nonce increase, gas payment, chain compatibility, etc.) and make interaction with blockchain more intuitive for end users. Additional attributes (e.g., event participation, proposal voting, etc.) could also be associated with an on-chain identity (i.e., a blockchain address) via Non-Fungible Tokens (NFTs) [26] or Soulbound Tokens (SBTs) [27]. Those attributes might be required for certain dApps (e.g., token airdrop).

5.1.2 Off-Chain Identity

In DePIN applications, an off-chain identity is required for establishing trusted person-to-machine and machine-to-machine relationships. While a digital certificate (e.g., X.509) , which binds an identity to a public key, is widely used to enable trust in a centralized system, self-sovereign identity (SSI) [48] provides a promising identity solution for securing communications between two entities in a decentralized setting. As illustrated in Figure 5.1, SSI is composed of three key pillars, namely decentralized identifiers (DIDs) [49], verifiable credentials (VCs) [51] and DIDComm messaging [50]. Once each participant (i.e., person or machine) in a decentralized system registers its DID on a verifiable data registry (e.g., blockchain), two entities can establish a secure communication channel and authenticate with each other by exchanging DIDComm messages. VCs come in handy when additional identity attributes are required to be attested by certain entities (i.e., VC issuers).

5.2 The ioID Design

ioID, which leverages blockchain wallet addresses (either Externally Owned Account (EOA) or Account Abstraction (AA) wallet) as on-chain identities and DIDs as off-chain identities, is a unified identity system designed by IoTeX for handling on-chain and off-chain digital relationships among participants in DePIN applications. As a general-purpose identity system, we envision that ioID could

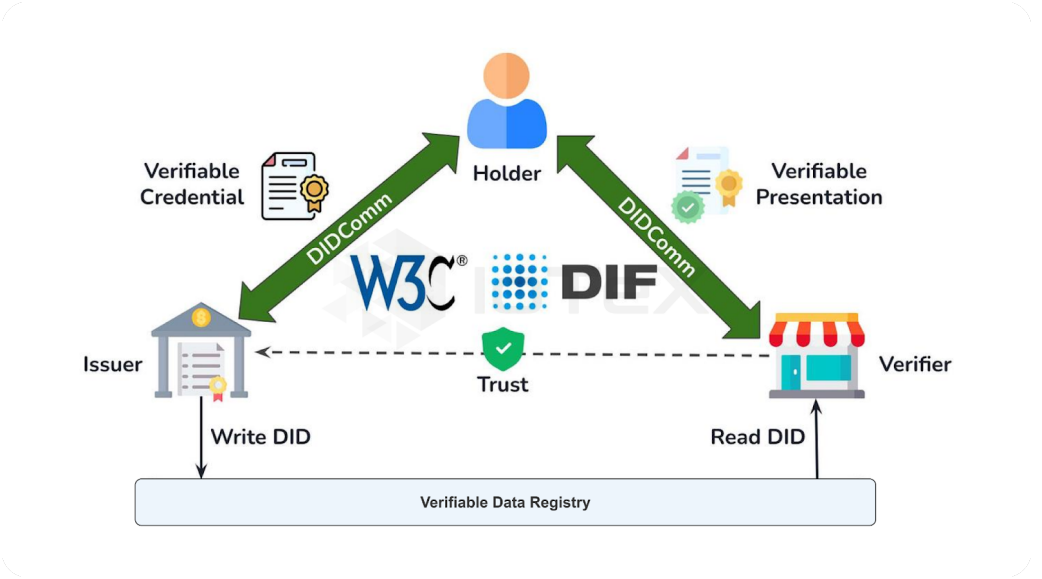

Figure 5.1: The Three Key Pillars of SSI

be utilized in different layers of the DePIN modular infrastructure, as shown in Figure 5.2.

5.2.1 On-Device ioID Generation

A DePIN device is able to generate a DID and the corresponding DID document on-the-fly within the device by integrating the IoTeXâs ioConnect SDK [16]. For a DePIN node deployed to support operation of a certain centralized or decentralized layer in a modular DePIN stack, a node operator could generate a DID and DID document using a command-line interface (CLI). For embedded DePIN devices, manufacturers could integrate the ioConnect SDK into the device firmware and allow users to read a DID and DID document (e.g., via serial ports) from devices.

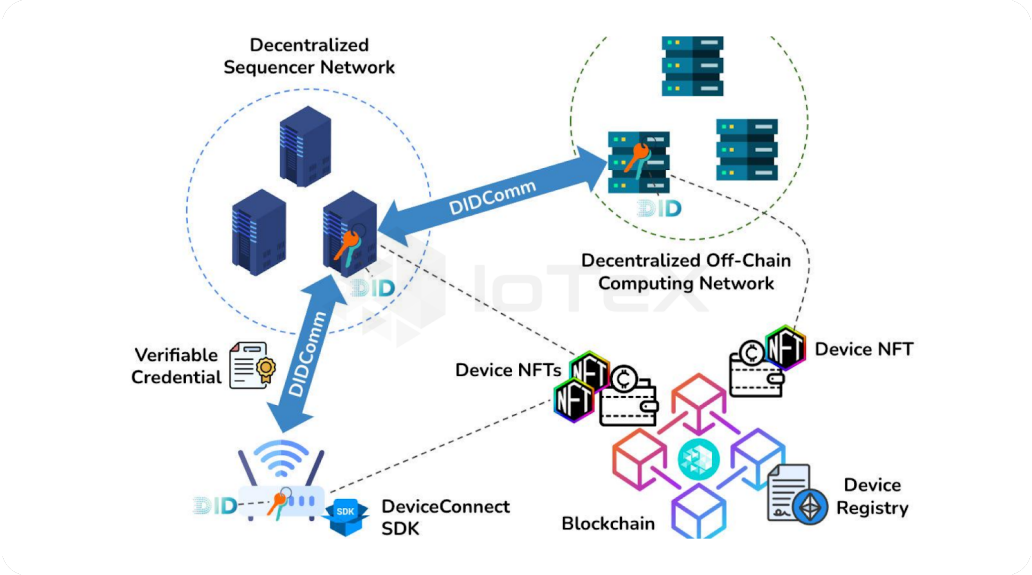

Figure 5.2: An Overview of the ioID Identity System

5.2.2 On-Device ioID Generation

A DePIN device owner can onboard a device via a web portal (e.g., the IoTeXâs MachineFi Portal). The onboarding process is shown in Figure 5.3.

1. A device owner first logs into the web portal using Metamask;
2. The device owner makes a minimum token deposit (e.g., 10 IOTX tokens) on the web portal. Those tokens are used for paying gas fees during the device onboarding process;
3. The device owner obtains a DePIN deviceâs DID and DID Doc:
   (a) For a DePIN node, the device owner (i.e., a node operator) needs to log into a node locally or remotely and uses the CLI to generate a DID and the corresponding DID Doc on the node;
   (b) For an embedded DePIN device, the device owner needs to
      i. Connect the device to PC via USB;

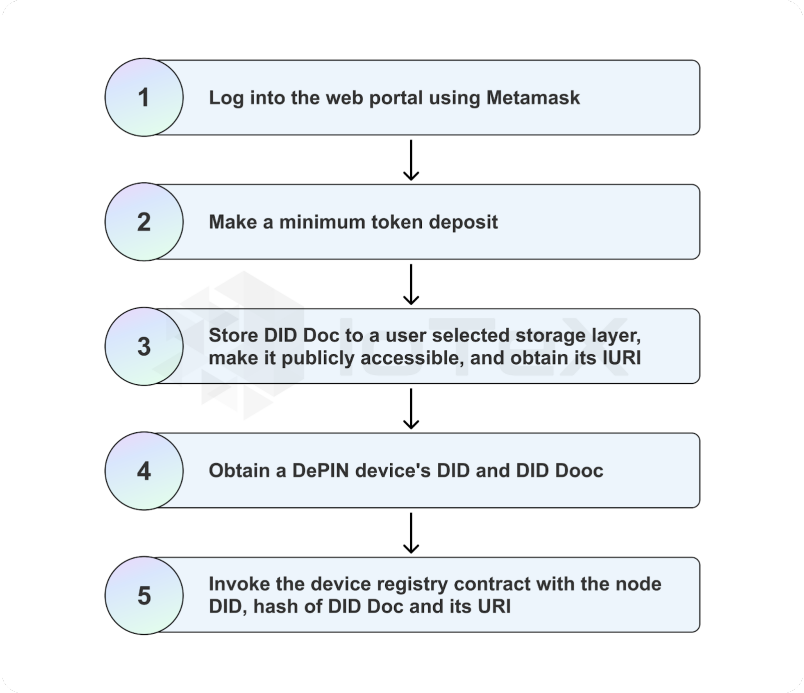

Figure 5.3: A Miner's Journey for Onboarding DePIN Devices

ii. Click "Read Device DID & DID Doc" button on the web portal to retrieve the deviceâs DID and DID Doc via the serial port;

4. The device owner selects a centralized or decentralized storage layer provider (e.g., AWS S3, IPFS, etc.), stores the DID Doc, makes it publicly accessible, and obtains its URI;

5. The device owner invokes the device registry contract with the deviceâs DID, hash of the DID Doc, and URI of the DID Doc.

After a successful device onboarding process, a DePIN device owner is able to see a device NFT shown in his/her blockchain wallet, which represents on-chain ownership of a DePIN device.

5.2.3 Secure Machine-to-Machine Interactions

Once a DePIN deviceâs DID is registered on-chain during the device onboarding process, it is able to conduct secure off-chain communications with other entities in the network based on the standardized DIDComm messaging protocol.

5.3 Integration of ioID in a DePIN Project

A DePIN project needs to complete a number of setups before using the ioID module.

5.3.1 Smart Contracts in ioID

The ioID suite of smart contracts provides a robust framework for decentralized identity management on the IoTeX blockchain. These contracts collectively provide a robust framework for identity management and interaction within the IoTeX ecosystem.

- **DePIN Project Registry**: The DePIN Project Registry is an NFT-based registry that manages all DePIN projects. It ensures that each project is uniquely identified and authenticated within the network.
- **ioID NFT Contract**: The ioID NFT contract is an essential part of the ioID framework for decentralized identity management on the IoTeX blockchain. It's directly managed by the Project Registry and is in charge of creating and assigning unique ioID tokens for devices. This involves linking devices to project IDs and owners, and generating associated wallet addresses according to the ERC6551 standard.
- **ioID Store**: The ioID Store is responsible for managing the application and activation of ioID across all projects. It handles the lifecycle of identity management applications, ensuring that identities are correctly set up and maintained.

- **ioID Registry**: The ioID Registry contract is used for registering devices on-chain and activating their ioID. It also serves as a DID resolver, providing a reliable means for verifying device identities across different projects.

5.3.2 Deploying the Device NFT Contract

To integrate a DePIN project with the IoTeX ioID module, the project owner starts by deploying a "Device NFT" contract to tokenize each device within their project. A user who owns a device NFT from a DePIN project is entitled to register a new ioID identity for a physical device and bind it to their blockchain wallet. When a new ioID is registered for a device, an ioID NFT is minted to the owner's wallet, and the corresponding device NFT is transferred to the ERC-6551 wallet of the ioID. This process effectively "activates" the ioID, linking the physical device to its digital identity and to its owner on the blockchain.

5.3.3 Registering a DePIN Project

Any DePIN project intending to use ioID identities must apply for a certain number of ioIDs by paying the required amount. ioIDs can only be requested by registered DePIN projects on the IoTeX blockchain. A project owner can either make a direct smart contract call or use the IoTeX command line interface (i.e., ioctl) to register a DePIN project. Once the transaction is completed you will receive a Project NFT with a certain Token ID, representing your DePIN Project ID on the IoTeX blockchain.

5.3.4 Setting the Device NFT Contract

After registering a DePIN project, the next step is to set the Device NFT contract for that project in the ioID Store. This contract must be set before a device attempts to register an ioID for your project. A project owner can either make a direct smart contract call or use the IoTeX command line interface (i.e., ioctl) to complete this step.

5.3.5 Requesting ioIDs

A project owner needs to apply for ioIDs by paying the required amount of IOTX tokens. The amount is determined by the number of ioIDs requested. The project owner can either make a direct smart contract call or use the IoTeX command line interface (i.e., ioctl) to request ioIDs. After the transaction, the number of requested ioIDs will be associated with the DePIN project.

5.3.6 Registering a Device

After setting the Device NFT contract and requesting a certain number of ioIDs for a DePIN project, physical devices can now be activated for the project by registering them in the ioIDRegistry contract. This process is performed by the device owner and will mint a new ioID NFT to the device owner's account, bind it to the device's DID and to the Device NFT.

Chapter 6

ioConnect - A Universal Embedded SDK for Empowering Device Abstraction

DePIN applications involve diversified hardware devices with different capabilities and functionalities. The primary goal of the Hardware Abstraction Layer (HAL) in the modular DePIN infrastructure is to abstract the complexity and heterogeneity of a wide range of smart devices (big or small) and facilitate them to connect with a centralized or decentralized Connectivity Layer (CL) in a secure manner, as illustrated in Figure 6.1. A challenging question is designing a universal embedded SDK that allows device manufacturers to connect their devices to a DePIN backend easily. In practice, ioConnect SDK aims to support popular microcontroller families (e.g., ESP32, Arduino, STM32, etc.), single-board computers (e.g., Raspberry Pi, ODROID, Rock Pi, etc.), and smartphones (e.g., Android and iOS) is highly desirable.

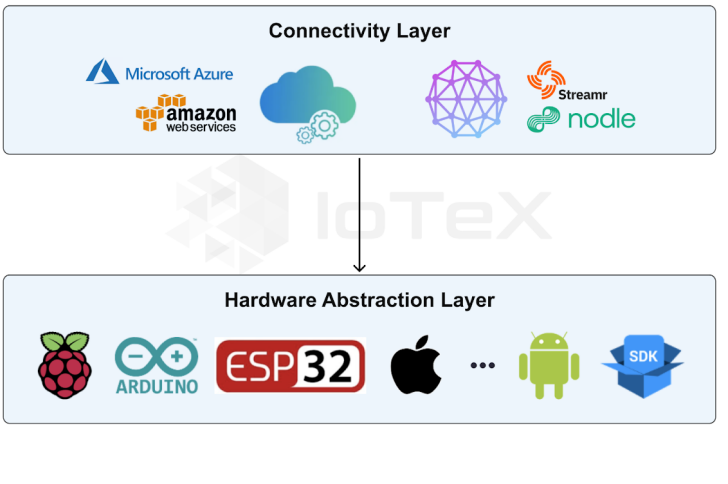

Figure 6.1: Secure Connection between HAL and CL

6.1 Connectivity Options

6.1.1 Connecting to a Centralized Connectivity Layer

Connecting a smart device to a centralized connectivity layer (e.g., a cloud-based IoT gateway) has been extensively investigated in the traditional IoT industries and adopted by quite a few early-stage DePIN projects due to its technology maturity. Digital certificates (e.g., X.509) are often utilized to ensure secure communication between smart devices and a centralized connectivity layer. Using a cloud-based IoT gateway (e.g., AWS IoT Core [46]) as an example (see Figure 6.2), a user can first create a digital twin in the cloud and generate a device certificate. Once the certificate is installed in a smart device, it can establish a secure TLS connection with the cloud-based IoT gateway. The digital twin then interacts with other services in the cloud on behalf of the smart device.

A centralized connectivity layer, while simplifying the device connection and management, represents a single point of failure in a DePIN application and the adoption of a decentralized connectivity layer should be seriously considered by

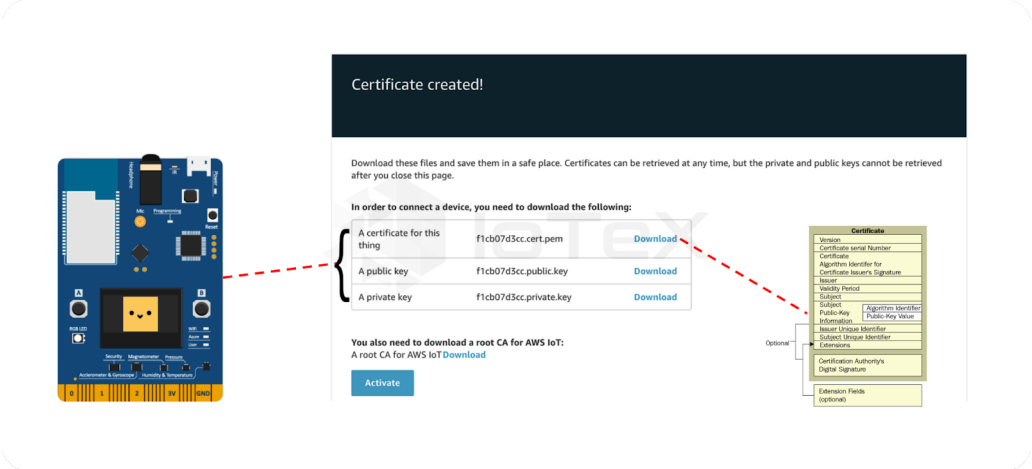

Figure 6.2: Device Onboarding with AWS IoT Core

future DePIN projects.

6.1.2 Connecting to a Decentralized Connectivity Layer

While a decentralized connectivity layer offers a more robust network connection for a DePIN application, connecting a smart device to it introduces a number of technical challenges:

- How can a smart device securely connect with nodes in the decentralized connectivity layer without relying on a centralized certificate authority (CA) and digital certificates?
- How can a smart device mutually authenticate with nodes in the decentralized connectivity layer?
- How can a smart device establish a secure channel with nodes in the decentralized connectivity layer?

To address the aforementioned technical challenges, a DePIN device should realize new technology and protocols that could be used in such a decentralized setting.

6.2 Design Considerations for Building a Universal Embedded SDK for DePIN Devices

The potential challenges of connecting a wide range of smart devices to a decentralized connectivity layer have led to the following design requirements towards developing a universal embedded SDK for DePIN devices:

- The SDK should accommodate popular hardware chipsets and platforms (e.g., microcontrollers, single board computers, smartphones, etc.);
- The SDK should be easily integrated by DePIN device manufacturers into their devices;
- The SDK should allow DePIN devices to use advanced security functionalities (e.g., secure elements, cryptography accelerators, etc.);
- The SDK should enable a DePIN device to establish a trusted relationship with other entities (i.e., people or machines) in a decentralized setting.

Those design requirements have motivated us to explore emerging technologies such as Armâs PSA certified crypto API and self-sovereign identity (SSI) as well as a layered SDK design methodology.

6.2.1 Arm's PSA Certified Crypto API

The Arm's PSA certified crypto API [47] defines standardized and unified interfaces for accessing cryptographic operations and key management services on a wide range of hardware platforms. By loading a cryptographic software/hardware driver available on a target hardware platform, a developer can easily access all the security-related functionalities via the PSA crypto API, as shown in Figure 6.3.

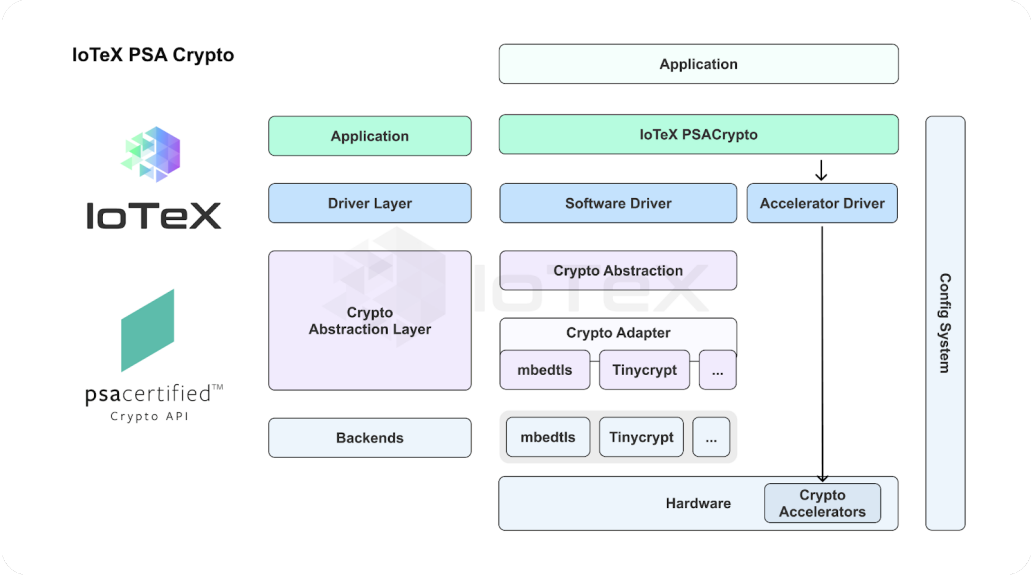

Figure 6.3: The Usage of IoTeXâs PSACrypto Library in DePIN Devices

The integration of the Armâs PSA certified crypto API into DePIN devices can potentially enhance security of DePIN devices, thereby mitigating increasing fraud risks in DePIN applications effectively.

6.2.2 Self-Sovereign Identity (SSI)

Self-sovereign identity (SSI) [48] techniques, such as Decentralized Identifiers (DIDs) [49], Verifiable Credentials (VCs) [51] and DIDComm messaging [50], move control of digital identity from conventional identity providers to individuals and lay down the foundation for people, organizations and things forming rich digital relationships. In a decentralized setting, SSI provides a promising solution for establishing trusted person-to-machine and machine-to-machine relationships without relying on third-party centralized or federated identity providers, as illusated in Figure 6.4.

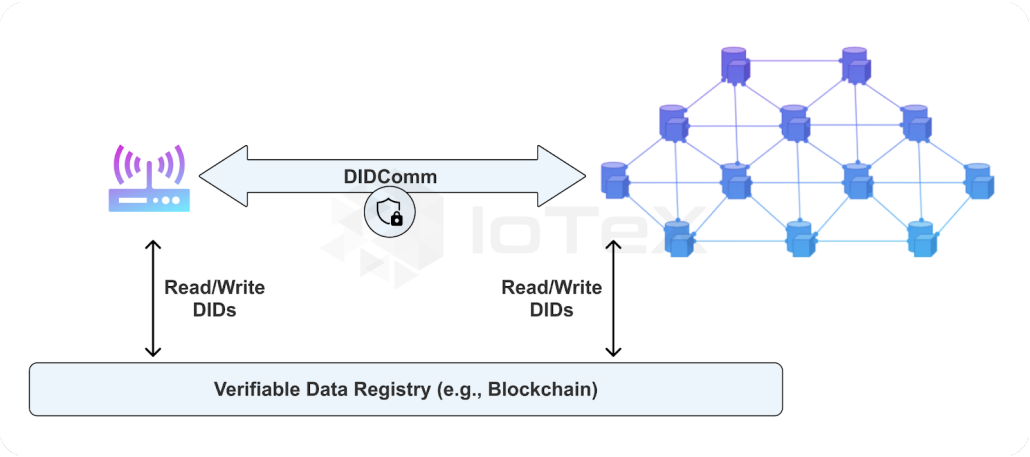

Figure 6.4: SSI-Based Communication in a Decentralized Setting

6.3 Implementation Specification

ioConnect [16] is a universal embedded SDK dedicatedly designed by IoTeX for empowering DePIN devices. To support a wide range of smart devices and application requirements, the SDK is architectured with a SDK core and a platform adaption layer (PAL).

6.3.1 ioConnect SDK Core

The core of ioConnect consists of four layers as shown in Figure 6.5. The bottom two layers realize the Armâs PSA certified crypto API specification v1.1, whereas the top two layers implement the three key pillars (i.e., DIDs, VCs and DIDComm) in SSI. All the cryptographic operations required in SSI are done through the PSA crypto API calls.

Note that the ioConnect SDK core is independent of hardware platforms and does not bind to specific components/resources on a DePIN device.

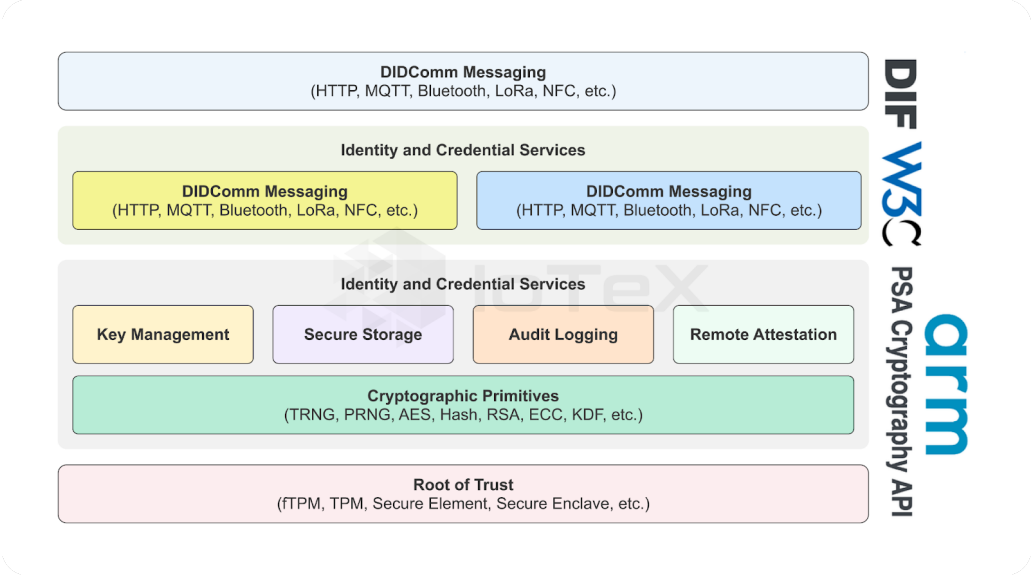

Figure 6.5: The ioConnect SDK Core

6.3.2 DePIN Device Compatibility

To accommodate a wide range of DePIN devices, the entire ioConnect SDK adopts a layered design methodology as illustrated in Figure 6.6. On the one hand, the Core contains the implementations of hardware independent specifications (e.g., SSI, PSA crypto API, etc.), the Platform Adaption Layer (PAL) deals with the differences among various embedded systems and platforms (e.g., compilation rules, coding conventions, framework design, etc.).

The introduction of PAL allows developers to easily add new hardware support by simply developing another PAL component with only 300 to 500 lines of code, thereby effectively addressing the DePIN device compatibility issue and significantly reducing integration complexity of DePIN device manufacturers.

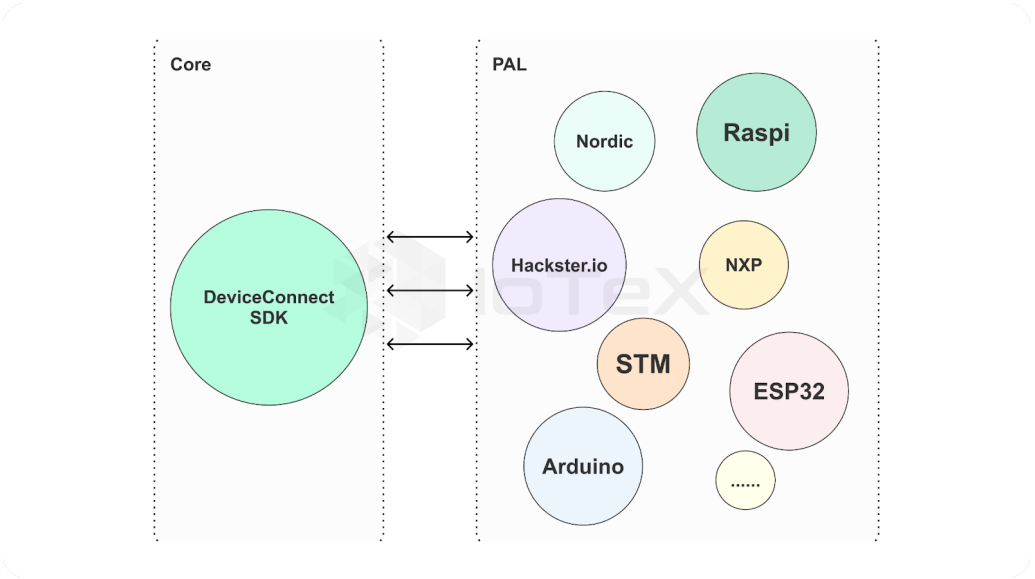

Figure 6.6: The Layered Architecture in the ioConnect SDK

Chapter 7

ioDDK - Enabling Self-Sovereign DePIN App Chains

7.1 Design Rationale

The rationale behind enabling application-specific L2s for DePIN projects on IoTeX L1 is driven by several compelling factors.

- Firstly, application-specific L2s are crucial for DePIN projects because they allow for the introduction of unique tokenomics, tailored user experiences (e.g., wallet and browser), and customized governance structures. This customization is vital for optimizing the blockchain to meet the specific needs and scenarios of each DePIN application at scalability, ensuring that each project can achieve its full potential.
- Additionally, many DePIN projects lack the expertise and financial resources required to build and maintain their own blockchain infrastructure.

As of now, the IoTeX L1 is secured by a pool of 120+ globally distributed delegates (i.e., validators) through our in-house Randomized Delegated Proof-of-Stake (Roll-DPoS) consensus protocol [52]. By leveraging the secure blockspace

from the IoTeX L1, these DEPIN projects can seamlessly launch their application-specific L2s without the heavy lifting associated with blockchain development.

ioDDK is a chain SDK that allows DePIN projects to provision self-sovereign application chains and inherit the security of IoTeX L1 simultaneously, as illustrated in Figure 7.1. While validating and proposing IoTeX L1 blocks, validators also reach consensus on transactions from DePIN application chains. By renting out blockspace, the IoTeX L1 can provide DePIN projects with the necessary resources to deploy their tailored solutions efficiently, without the need for significant upfront investments or technical know-how, fostering a more vibrant and innovative ecosystem.

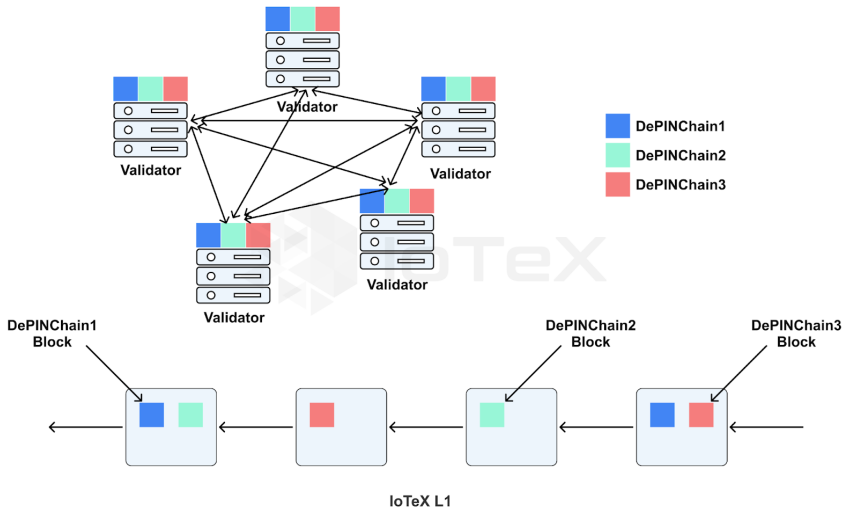

Figure 7.1: Self-Sovereign DePIN App Chains Secured by IoTeX L1

7.2 Shared Blockspace and Validators

To minimize development complexity, all self-sovereign DePIN chains can share blockspace and validators with IoTeX L1. Three implementation options could be considered in practice, as illustrated in Figure 7.2.

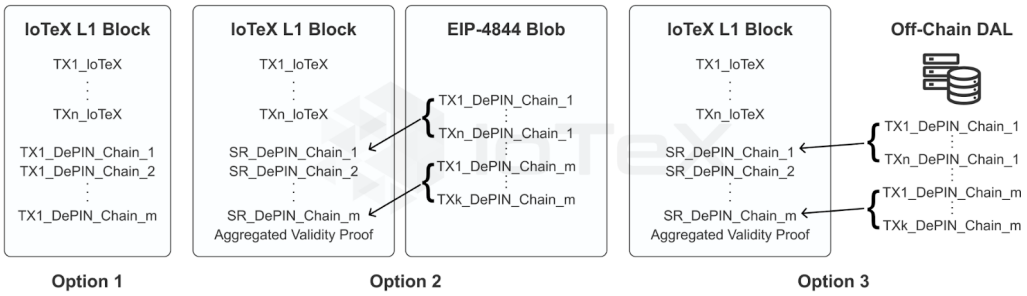

Figure 7.2: Three Implementation Options for Shared Blockspace and Validators

Option 1 - Storing All Transactions on IoTeX L1

In this option, transactions from self-sovereign DePIN chains together with those on IoTeX L1 share the same blockspace and all transactions need to go through the consensus process of IoTeX L1. This approach ensures that all self-sovereign DePIN chains achieve the same security as IoTeX L1. However, due to the limitation of block size, only a certain number of DePIN projects can be supported. A decentralized governance process might be required to determine which DePIN projects are eligible for using this approach.

Option 2 - Storing DePIN Chain Transactions using EIP-4844

In this option, transactions from self-sovereign DePIN chains are temporarily stored on IoTeX L1 using EIP-4844 blobs. The state roots together with an aggregated validity proof of state transitions of all self-sovereign DePIN chains share the same blockspace with IoTeX L1 transactions. The aggregated validity proof is verified on IoTeX L1 to settle all the transactions on self-sovereign DePIN chains. Such a rollup-based approach can effectively improve system scalability and allow all self-sovereign DePIN chains to inherit the security of IoTeX L1 simultaneously. Note that one of provers in the W3bstream network should be utilized to realize this approach.

Table 7.1: Comparison of Three Implementation Options

	DePIN Chain Transaction Storage	Scalability	W3bstream Need	Security
Option 1	on-chain block	Low	No	High
Option 2	on-chain blob	High	Yes	High
Option 3	off-chain DAL	High	Yes	Low/Medium

Option 3 - Storing DePIN Chain Transactions using Off-Chain DAL

In this option, self-sovereign DePIN chains can choose an off-chain data availability layer (DAL) for storing their transactions. Similar to the Option 2, the state roots together with an aggregated validity proof of state transitions of all self-sovereign DePIN chains share the same blockspace with IoTeX L1 transactions. The aggregated validity proof is verified on IoTeX L1 to settle all the transactions on self-sovereign DePIN chains. However, the state roots should be committed to the IoTeX L1 by the DAL in this approach. While such a validum-based approach can also improve system scalability, the security depends on that of the implementation of a specific DAL. Note that one of provers in the W3bstream network should be utilized to realize this approach.

Comparison of Three Options

Table 7.2 provides a comparison of the above three implementation options with respect to the DePIN chain transaction storage, scalability, W3bstream requirement and security.

7.3 ioDDK Components and High-Level Workflow

7.3.1 ioDDK Components

ioDDK, which enables a DePIN project to leverage the existing delegates (i.e., validators) and blockspace in IoTeX L1 to host a self-sovereign DePIN chain, consists of the following components:

- **Chain Configuration**: The chain configuration component allows a developer to configure the specific parameters (e.g., start height, transaction type, blockspace requirement, etc.) of a DePIN chain;
- **Chain Deployment**: The chain deployment component allows a developer to manage the deployment process of a DePIN chain across all the delegates of IoTeX L1;
- **Chain Explorer**: The chain explorer component allows a DePIN project as well as external parties to monitor the status and key metrics (i.e., block height, TPS, transaction details, etc.) of a DePIN chain;
- **Chain Commander**: The chain commander is a command line tool that provides a suite of commands to simplify the development and management of a DePIN chain.

7.3.2 High-Level Workflow

Once a DePIN project is approved for provisioning a self-sovereign chain using the shared blockspace and validators in IoTeX L1 (e.g., via a decentralized governance process), the project can use ioDDK as follows:

- The developer uses the “Chain Configuration" function in ioDDK to specify a number of DePIN chain specific parameters:

  - **chainID**: a chain identifier is generated automatically to represent the self-sovereign DePIN chain;
  - **Transaction type**: the different fields in a transaction;
  - **Maximum transaction numbers**: the maximum number of DePIN chain transactions processed in a IoTeX L1 block;
  - **W3bstream prover**: the selection of a W3bstream prover.
- The developer prepares a docker image of the transaction processing logic for a DePIN chain and uses the âChain Deploymentâ function in ioDDK to deploy the docker image to all the delegates of IoTeX L1.

Once the DePIN chain specific transaction processing logic is deployed to IoTeX L1 delegates, the DePIN chain transactions will be processed accordingly. The developer can use âChain Explorerâ in ioDDK to check the status of the provisioned DePIN chain. Moreover, the developer can also use the âChain Commanderâ to manage the DePIN chain using a number of support commands.

7.4 The Marketplace for Renting Blockspace

We plan to implement a blockspace marketplace enabling developers to trade blockspace tailored for their specific DePIN L2s built with ioDDK. This market-oriented strategy ensures that resource allocation adapts to real-time demand, thereby optimizing the network's overall efficiency.

The introduction of tradable blockspace also impacts the utility and liquidity of the IOTX token. For example, developers can stake or burn IOTX to get a certain amount of blockspace. Revenue generated from transactions can be allocated in multiple ways, including funding the treasury or being burnt to regulate token supply.

7.5 Implication on the IoTeX L1

The introduction of shared blockspace to IoTeX L1 brings a host of features designed to meet the growing demands of DePIN L2 projects:

- **Fast Block Time and Finality**: One of the primary requirements for DePIN L2s is a fast block time with quick finality to optimize user experience. Currently, IoTeX L1 has a block time of 5 seconds. However, to meet the needs of high-performance DePIN projects, we aim to reduce this block time to 2 seconds. This reduction will significantly enhance the responsiveness and efficiency of L2 applications, ensuring a smoother and more user-friendly experience.
- **Increased Throughput and Decentralization**: The total throughput of DePIN L2s is inherently limited by the computer power of all validators in the IoTeX L1 network. To address this, it is crucial to both increase the number of validators and improve the overall decentralization of the network. By expanding the validator pool, IoTeX L1 can support a higher transaction volume and provide more robust security. This enhancement will also facilitate a more decentralized and resilient network, essential for maintaining trust and stability in a growing ecosystem.

To fulfill the above requirements, the introduction of Proposer-Builder Separation (PBS) [53] is planned. PBS is a concept originally proposed by Ethereum researchers designed to enhance the censorship resistance and overall performance of blockchain networks. It separates the roles of block proposers and block builders to optimize block production and ensure fairness in the validation process.

- **Block Proposers**: Responsible for proposing new blocks based on the current state of the blockchain and network rules. They gather transactions and create a block proposal that will be validated by the network. This role will most likely be filled by the current consensus delegates.

- **Block Builders**: Specialized entities focused on constructing blocks by selecting the most valuable transactions from the actpool, optimizing block space usage, and potentially enhancing throughput. They submit their constructed blocks to proposers, who then propose these blocks to the network for validation. This will be a new role introduced to the IoTeX L1 network and dedicatedly to work on package transactions including those from DePIN L2s.

The separation of these roles helps mitigate the risk of centralized control and censorship by distributing responsibilities across different entities. This improves network capacity and reduces transaction processing time, i.e., it also allows for more efficient block production, as builders can focus on transaction selection, optimization and even sharding, while proposers handle the consensus and block finalization processes. This approach will ensure that DePIN L2s that based the shared blockspace provided by the IoTeX L1 can operate efficiently and securely, meeting the demands of their specific application scenarios.

Chapter 8

The New Roadmap

IoTeX 2.0 is a collection of numerous components that we plan to build from now until 2026. The roadmap is provided below in Figure 8.1. Note that many of the components listed are dependent on governance proposals and voting, and are therefore subject to change.

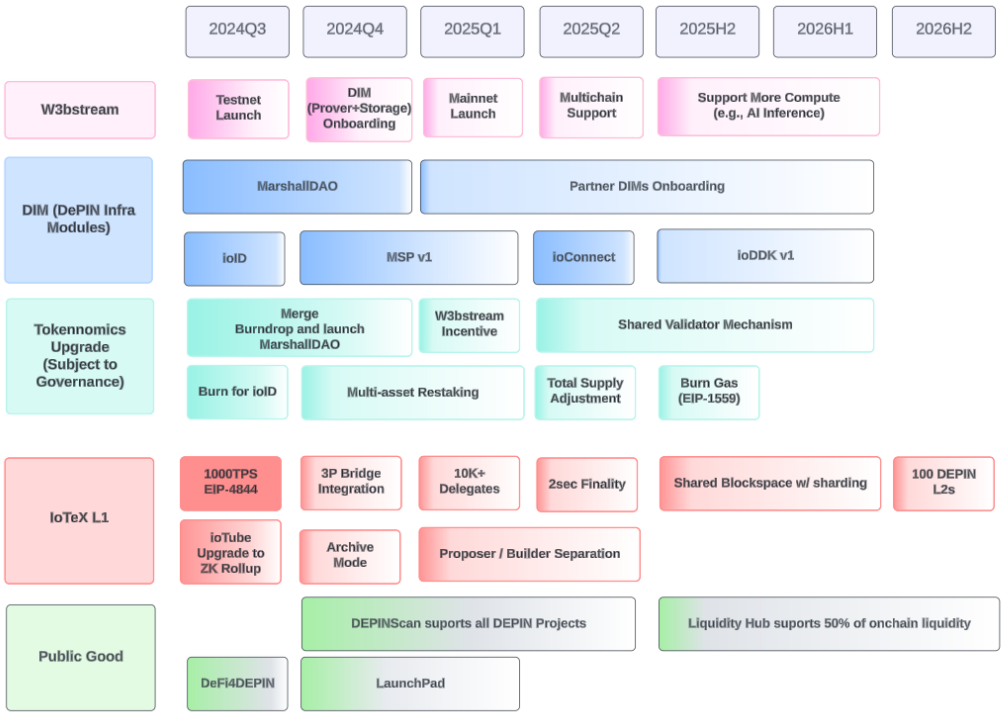

Figure 8.1: IoTeX 2.0 Roadmap

Chapter 9

Conclusion

IoTeX 2.0 offers a new vision for the IoTeX Network while preserving the core principles that led to its inception. From the beginning, IoTeX has envisioned a future where individuals can own and control their devices, as well as the data and value these devices produce. IoTeX aims to be a hub for real-world, real-time data, powering a superintelligent AI network. This network won't just exceed human intelligence but will leverage precise and reliable data that reflects the real world in real-time. This shift suggests that ultimate truth and decision-making power will be rooted in the tangible, dynamic realities of our physical environment. This transformation changes how data is valued and used, influencing the future of civilization. Most importantly, everything IoTeX enables will be owned and operated by the people, for the people.

Thank you to the IoTeX community for your continued contributions, support, and feedback. As we embark on this new ambitious journey, we know that IoTeX and our global community will enact real change and bring DePIN to every country in the world. It's time to build!

Disclaimer

This whitepaper is a collaborative effort by IoTeX coredev and members from the IoTeX community. It outlines a proposed direction for the IoTeX Network. However, the contents do not entail a commitment by any authors or their respective organizations. The IoTeX community is responsible for adapting and adopting the measures proposed in this paper. The success of any proposal will ultimately depend on the hard work of the wider community and those building within the IoTeX Network.

The information presented herein is provided by the parties listed above (the PARTIES) for informational purposes only. Neither the PARTIES nor any of their affiliates, directors, officers, managers, employees, or representatives make any representations or warranties, expressed or implied, regarding any of the material or information contained herein. Furthermore, the PARTIES or any such individuals do not assume or have any responsibility or liability to you or your affiliates, or your or your affiliates' respective directors, officers, managers, employees, or representatives resulting from the use of the information and material contained herein.

The information provided here is supplied in good faith based on believed information, but it is not guaranteed to be accurate or complete. The information in this paper should not be considered as investment advice, financial advice, trading advice, or any other form of advice. It is recommended that you conduct your own due diligence and consult with your financial advisor before making any investment decisions of any kind.

Acknowledgment

We extend our heartfelt gratitude to the following individuals and venture capital firms (i.e., Vinayak Kurup from Escape Velocity (EV3), Robert Koschig from 1kx, 6th Man Ventures (6MV), SNZ Capital, Future Money Group (FMG), Álvaro Gracia from Borderless Capital, Lattice, Summer Capital, Pantera Capital, BlueYard Capital, Spartan Capital, Lemniscap, NGC Ventures, Stanford Blockchain Accelerator, Foresight Venture, and Samsung NEXT), Web3 projects (i.e., NEAR Foundation, RISC0, Helium Foundation, The Graph Foundation, Filecoin Foundation, and Textile), and crypto research firms (i.e., IntoTheBlock (ITB) and Messari) whose invaluable feedback and unwavering support have been instrumental in shaping this Whitepaper. Your expertise, insights, and commitment have significantly enhanced the depth and quality of our work. We are deeply appreciative of the time and resources you have invested, and your contributions have been crucial in driving the IoTeX 2.0 mission forward.

Bibliography

[1] Pebble Tracker. https://docs.iotex.io/dev-toolkit/web3-smart-devices/pebble-tracker.

[2] X. Fan, Q. Chai, Z. Li, and T. Pan, "Decentralized iot data authorization with pebble tracker," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1-2.

[3] Ucam. https://ucam.iotex.io/.

[4] DePIN DevKit - SenseCAP Indicator D1. https://www.seeedstudio.com/SenseCAP-Indicator-D1-p-5643.html.

[5] IoTeX - A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain, The IoTeX Team, https://github.com/iotexproject/files/blob/main/publications/IoTeX_Whitepaper_1.5_EN.pdf, July 12, 2018.

[6] X. Fan, Z. Zhong, Q. Chai, and D. Guo, "Ucam: A User-Centric, Blockchain-Based and End-to-End Secure Home IP Camera System," in *Security and Privacy in Communication Networks*, N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Eds., Cham: Springer International Publishing, 2020, pp. 311â323.

[7] M. Brossard, G. Bryant, X. Fan, A. Ferreira, E. Grimley-Evans, C. Haster, D. Miller, D. P. Mulligan, H. J. M. Vincent, S. Xiong, and L. Xu, "Privacy-Preserving Object Detection with Veracruz", *PerCom Workshops 2023*, pp. 322-324, 2023.

[8] M. Brossard, G. Bryant, B. El Gaabouri, X. Fan, A. Ferreira, E. Grimley-Evans, C. Haster, E. Johnson, D. Miller, F. Mo, D. P. Mulligan, N. Spinale, E. Van Hensbergen, H. J. M. Vincent, and S. Xiong, "Private Delegated Computations Using Strong Isolation," *IEEE Trans. Emerg. Top. Comput*, 12(1): 386-398, 2024.

[9] IoTeX Foundation, The Building Blocks of DePIN, `https://iotex.io/blog/the-building-blocks-of-depin/`.

[10] IIP-23: The Marshall DAO, `https://community.iotex.io/t/iip-23-the-marshall-dao/11172`.

[11] N. Pippenger, "On the evaluation of powers and related problems," In *17th Annual Symposium on Foundations of Computer Science (sfcs 1976)*, pp. 258â263. IEEE Computer Society, 1976.

[12] D. J. Bernstein, J. Doumen, T. Lange, and J.-J. Oosterwijk, "Faster batch forgery identification," In *International Conference on Cryptology in India*, pp. 454â473. Springer, 2012.

[13] E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson, "Fast exponentiation with precomputation: Algorithms and lower bounds," preprint, 1995.

[14] G. Luo, S. Fu, G. Gong, "Speeding up multi-scalar multiplication over fixed points towards efficient zksnarks," *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023(2), pp. 358-380, 2023.

[15] X. Fan, V. Kuchta, F. Sica, and L. Xu, "Speeding Up Multi-Scalar Multiplications for Pairing-Based zkSNARKs," *Cryptology ePrint Archive, Paper 2024/750*, 2024, `https://eprint.iacr.org/2024/750`.

[16] ioConnect - A Universal Embedded SDK for Connecting Smart Devices to Web3. `https://github.com/machinefi/ioConnect`.

[17] W3bstream. `https://w3bstream.com/`.

[18] D. Patrick, DePIN Supercharged â Introducing the Worldâs First DePIN Accelerator. https://iotex.io/blog/depin-accelerator/.

[19] ioTube - A Decentralized Multi-Asset Cross-Chain Bridge. https://bridge.iotex.io/.

[20] ioPay - A DePIN Wallet. https://iopay.me/.

[21] DePIN Liquidity Hub. https://iotex.io/depin-liquidity.

[22] mimo - A Decentralized Exchange for Everyone. https://mimo.finance/.

[23] DePINscan. https://depinscan.io/.

[24] A. Basi, DePIN Liquidity Hub - Join the Fastest Growing Sector in Crypto, https://iotex.io/blog/depin-liquidity-hub/.

[25] V. Buterin, Y. Weiss, D. Tirosh, S. Nacson, A. Forshtat, K. Gazso, and T. Hess, ERC-4337: Account Abstraction Using Alt Mempool, Ethereum Improvement Proposals, 2021.

[26] W. Entriken, D. Shirley, J. Evans, and N. Sachs, ERC-721: Non-Fungible Token Standard, Ethereum Improvement Proposals, 2018.

[27] T. Daubenschütz and Anders, ERC-5192: Minimal Soulbound NFTs, Ethereum Improvement Proposals, 2022.

[28] Risc0. https://www.risczero.com/.

[29] Succinct Processor 1 (SP1). https://succinctlabs.github.io/sp1/.

[30] Nexus. https://www.nexus.xyz/.

[31] zkWasm. https://delphinuslab.com/zk-wasm/.

[32] Circom 2. https://docs.circom.io/.

[33] Halo 2. https://zcash.github.io/halo2/.

[34] ZoKrates. https://zokrates.github.io/.

[35] Noir. https://noir-lang.org/.

[36] Cairo. https://www.cairo-lang.org/.

[37] Intel Software Guard Extensions (SGX). https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html.

[38] Intel Trust Domain Extensions (TDX). https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html.

[39] AMD Secure Encrypted Virtualization (SEV). https://www.amd.com/en/developer/sev.html.

[40] AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More. https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/solution-briefs/amd-secure-encrypted-virtualization-solution-brief.pdf.

[41] AWS Nitro System. https://aws.amazon.com/ec2/nitro/.

[42] Arm Confidential Compute Architecture. https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture.

[43] G. Wuollet, Introducing the Nakamoto Challenge: Addressing the Toughest Problems in Crypto. https://a16zcrypto.com/posts/article/introducing-the-nakamoto-challenge-addressing-the-toughest-problems-in-crypto.

[44] IoTeX Foundation, Decentralized Verification in DePIN. https://iotex.io/blog/decentralized-verification-in-depin/.

[45] Modulus Labs, The Cost of Intelligence: Proving Machine Learning Inference with Zero-Knowledge. https://github.com/Modulus-Labs/Papers/blob/master/Cost_Of_Intelligence.pdf.

[46] AWS IoT Core. https://aws.amazon.com/iot-core/.

[47] Arm PSA Certified APIs. https://arm-software.github.io/psa-api/crypto/.

[48] Self-Sovereign Identity. https://en.wikipedia.org/wiki/Self-sovereign_identity.

[49] Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations. W3C Recommendation, 19 July 2022. https://www.w3.org/TR/did-core/.

[50] DIDComm Messaging. DIF Ratified Specification. https://identity.foundation/didcomm-messaging/spec/.

[51] Verifiable Credentials Data Model v1.1. W3C Recommendation, 03 March 2022. https://www.w3.org/TR/vc-data-model/.

[52] IoTeX Research, https://iotex.io/research.

[53] Vitalik Buterin, State of research: increasing censorship resistance of transactions under proposer/builder separation (PBS), https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance.